CENTURYLINK COMMUNICATIONS LLC DBA LUMEN TECHNOLOGIES GROUP

SOC 2 REPORT

FOR

COLOCATION SERVICES

A TYPE 2 INDEPENDENT SERVICE AUDITOR'S REPORT ON CONTROLS RELEVANT TO SECURITY AND AVAILABILITY

JUNE 1, 2021, TO MAY 31, 2022

PREPARED IN ACCORDANCE WITH THE
AICPA SSAE NO. 18 AND IAASB ISAE 3000 STANDARDS

Attestation and Compliance Services

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

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

TABLE OF CONTENTS

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To CenturyLink Communications LLC dba Lumen Technologies Group:

Scope

We have examined CenturyLink Communications LLC dba Lumen Technologies Group's ("Lumen" or the "service organization") accompanying description of its colocation services system, in Section 3, throughout the period June 1, 2021, to May 31, 2022, (the "description"), based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) ("description criteria"), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period June 1, 2021, to May 31, 2022, to provide reasonable assurance that Lumen's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability ("applicable trust services criteria") set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).*

Lumen uses various subservice organizations for aspects of the preventive maintenance and inspection services supporting environmental security systems at certain data center locations. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Lumen, to achieve Lumen's service commitments and system requirements based on the applicable trust services criteria. The description presents Lumen's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Lumen's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

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

Service Organization's Responsibilities

Lumen is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Lumen's service commitments and system requirements were achieved. Lumen has provided the accompanying assertion, in Section 2, ("assertion") about the description and the suitability of design and operating effectiveness of controls stated therein. Lumen is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA) and in accordance with International Standard on Assurance Engagements 3000 (Revised), Assurance Engagements Other Than Audits or Reviews of Historical Financial Information, issued by the International Auditing and Assurance Standards Board. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were

achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- Obtaining an understanding of the system and the service organization's service commitments and system requirements;
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively;
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria;
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria;
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria; and
- Evaluating the overall presentation of the description.

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

Service Auditor's Independence and Quality Control

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

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Test of Controls

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

Opinion

In our opinion, in all material respects,

a. the description presents Lumen's colocation services system that was designed and implemented throughout the period June 1, 2021, to May 31, 2022, in accordance with the description criteria;

b. the controls stated in the description were suitably designed throughout the period June 1, 2021, to May 31, 2022, to provide reasonable assurance that Lumen's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organizations applied the complementary controls assumed in the design of Lumen's controls throughout that period; and

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

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of Lumen; user entities of Lumen's colocation services system during some or all of the period of June 1, 2021, to May 31, 2022, business partners of Lumen subject to risks arising from interactions with the colocation services system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization;
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties;
- Internal control and its limitations;
- Complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements;
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services;
- The applicable trust services criteria; and
- The risks that may threaten the achievement of the service organization's service commitments and system requirements, and how controls address those risks.

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

Schellman & Company, LLC

Tampa, Florida
July 19, 2022

SECTION 2

MANAGEMENT'S ASSERTION

MANAGEMENT'S ASSERTION

We have prepared the accompanying description of Lumen's colocation services system, in Section 3, throughout the period June 1, 2021, to May 31, 2022, (the "description") based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), ("description criteria"). The description is intended to provide report users with information about the colocation services system that may be useful when assessing the risks arising from interactions with Lumen's system, particularly information about system controls that Lumen has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability ("applicable trust services criteria") set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

Lumen uses various subservice organizations for and aspects of the preventive maintenance and inspection services supporting environmental security systems at certain data center locations. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Lumen, to achieve Lumen's service commitments and system requirements based on the applicable trust services criteria. The description presents Lumen's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Lumen's controls. The description does not disclose the actual controls at the subservice organizations.

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

a. the description presents Lumen's colocation services system that was designed and implemented throughout the period June 1, 2021, to May 31, 2022, in accordance with the description criteria;

b. the controls stated in the description were suitably designed throughout the period June 1, 2021, to May 31, 2022, to provide reasonable assurance that Lumen's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations applied the complementary controls assumed in the design of Lumen's controls throughout that period; and

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

SECTION 3

DESCRIPTION OF THE SYSTEM

OVERVIEW OF OPERATIONS

Company Background

Lumen (NYSE: LUMN) is an outsourcing provider of managed computing and network infrastructure for IT applications. With customers in more than 60 countries and a focus on the customer experience, Lumen serves as its customers' trusted partner, helping them manage increased network and IT complexity and providing managed network and cyber security solutions that help protect their business.

Lumen infrastructure extends to 60 countries around the world and includes:

- 22,000 fully managed circuits in a private network supporting multiple application service levels
- Tier-1 OC-192 Internet backbone

Description of Services Provided

Lumen's facilities house premium space built according to uniform environmental and security standards for power, cooling, fire suppression, security, and easy access to overhead and raised-floor cabling. Its services are a component of user entities' information infrastructure and IT operations. As such, Lumen's services support the confidentiality, integrity, and availability of user entities' administrative, operational, and financial reporting information systems. User entities engage Lumen to secure and maintain the physical availability of their applications and important data for their customers, employees, and stakeholders.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Lumen has committed to customers to carry out certain objectives in relation to the services provided. These commitments are documented and formally reviewed by management as part of the risk assessment to ensure that the operations, reporting, and compliance objectives are aligned with the commitments and company's mission and risks to achieving commitments are identified and addressed.

Lumen's commitments to their customers related to security and availability are communicated via standard service level agreements (SLAs), the data center user guide, and customer contracts. Lumen's commitments include the following:

- Implement and continuously monitor physical security controls throughout data center facilities to safeguard customer systems and data.
- Implement and continuously monitor environmental monitoring systems and remediate events that may impact system availability.
- Implement redundant infrastructure to support the services.
- Perform preventative maintenance for environmental and power systems supporting the colocation services.

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

- Badge access control and video surveillance systems designed to restrict and monitor physical access to colocation facilities and protect customer's equipment.
- Dedicated physical security operations center (PSOC) personnel are staffed 24x7x365 to monitor and respond to physical security events.

- Fire detection and suppression systems (e.g., fire, heat, and smoke detectors, water sprinklers and/or gas suppression systems, etc.) to help ensure availability of systems.
- Redundant backup power supply systems (e.g., uninterruptible power supply (UPS) systems and/or generators, etc.) to provide electricity in the event of a power outage.
- Dedicated cooling systems (e.g., computer room air conditioning (CRAC), heating ventilation and air conditioning (HVAC) units, chillers, etc.) to regulate temperature and humidity levels.
- Building management systems (BMS) in place to monitor the environmental conditions within the data centers and notify field operations personnel when predefined thresholds are exceeded.
- Field engineers and/or third-party specialists inspect the environmental and power management systems in accordance with the service guide.

In accordance with Lumen's assertion, and the description criteria, the aforementioned service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system and may therefore not fully address the specific service commitments and requirements made to all system users, in each individual case.

COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICE

System Boundaries

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

The scope of this report is limited to the colocation services provided by Lumen in the 70 data center facilities within the table below:

Data Center	Facility Address	Occupancy
Albany	10 Airline Drive Albany, New York, 12205, United States	Multi-tenant
Atlanta	180 Peachtree Street NW, 4th Floor Atlanta, Georgia, 30303, United States	
Aurora‡	14200 East Jewell Avenue Aurora, Colorado, 80012, United States	Lumen Only
Austin	4207 Smith School Road Austin, Texas, 78744, United States	Multi-tenant
Baltimore‡	300 West Lexington Street Baltimore, Maryland, 21201, United States	
Boise‡	619 W. Bannock Street Boise, Idaho, 83702, United States	
Boston	300 Bent Street Cambridge, Massachusetts, 02141, United States	
Bothell	22722 29th Drive SE Bothell, Washington, 98021, United States	
Charlotte (Airport Center)‡	5001 Airport Center Parkway Charlotte, North Carolina, 28208, United States	Lumen Only

Data Center	Facility Address	Occupancy
Charlotte (Rose Lake)	4021 Rose Lake Drive Charlotte, North Carolina, 28217, United States	Lumen Only
Chicago (Canal Street)	111 N. Canal Street Chicago, Illinois, 60606, United States	Multi-tenant
Chicago (Kingsbury Street)	900 N. Kingsbury Street, 1st Floor Chicago, Illinois, 60610, United States	
Chicago (Broadview)‡	2101 Roberts Drive Broadview, Illinois, 60155, United States	Lumen Only
Cincinnati	400 Pike Street Cincinnati, Ohio, 45202, United States	Multi-tenant
Cleveland	4000 Chester Avenue Cleveland, Ohio, 44103, United States	Lumen Only
Dallas	3180 Irving Boulevard Dallas, Texas, 75247, United States	
Denver‡	1850 Pearl Street Denver, Colorado, 80203, United States	
Detroit‡	1965 Porter Street Detroit, Michigan, 48216, United States	
El Paso	501 W. Overland Avenue El Paso, Texas, 79901, United States	
Emeryville	5000 Hollis Street Emeryville, California, 94608, United States	
Garden City‡	71 Clinton Road Garden City, New York, 11530, United States	Multi-tenant
Herndon (520 Van Buren)	520 Van Buren Street Herndon, Virginia, 20170, United States	
Herndon (524 Van Buren)‡	524 Van Buren Street Herndon, Virginia, 20170, United States	Lumen Only
Houston	12001 North Freeway Houston, Texas, 77060, United States	
Jacksonville	4814 Phillips Highway Jacksonville, Florida, 32207, United States	
Kansas City	1212 E 19th Street Kansas City, Missouri, 64108, United States	
Lachine (Montréal)	4825 Francois Cusson Lachine, Quebec, H8T1V, Canada	
Las Vegas	1 Aerojet Way North Las Vegas, Nevada, 89030, United States	Multi-tenant
Little Rock‡	300 S. Gaines Little Rock, Arkansas, 72201, United States	Lumen Only
Indianapolis	1902 S East Street Indianapolis, Indiana, 46225	
Los Angeles	818 W. 7th Street, Suite 1100 Los Angeles, California, 90017, United States	Multi-tenant

Data Center	Facility Address	Occupancy
McLean‡	1755 Old Meadow Road McLean, Virginia, 22102, United States	Lumen Only
Metairie	3220 Lausat Street Metairie, Louisiana, 70001, United States	
Miami (5th St)	49 NW 5th Street Miami, Florida, 33128, United States	Multi-tenant
Miami (9th St)	50 NE 9th Street Miami, Florida, 33132, United States	
Minneapolis	511 11th Avenue South Minneapolis, Minnesota, 55415, United States	
Minnetonka (5480)	5480 Feltl Road Minnetonka, Minnesota, 55343, United States	Lumen Only
Minnetonka (5500)	5500 Feltl Road Minnetonka, Minnesota, 55343, United States	Multi-tenant
Nashville (9th Avenue)	2208 9th Avenue North Nashville, Tennessee, 37208, United States	Lumen Only
Nashville (Sidco Drive)‡	2990 Sidco Drive Nashville, Tennessee, 37204, United States	
Newark‡	165 Halsey Street, 7th floor Newark, New Jersey, 07102, United States	Multi-tenant
New York City (8th Ave)†	111 8th Avenue New York, New York, 10011, United States	
New York City (10th Ave)	85 10th Avenue, Suite 600 New York, New York, 10011, United States	
New York City (26th St)	601 W. 26th Street New York, New York, 10001, United States	
Omaha†‡	6805 Pine Street Omaha, Nebraska, 68106, United States	
Orlando	380 S. Lake Destiny Road Orlando, Florida, 32810, United States	Lumen Only
Philadelphia‡	401 N. Broad Street, Suite 310 Philadelphia, Pennsylvania, 19108, United States	Multi-tenant
Phoenix	811 S. 16th Street Phoenix, Arizona, 85034, United States	Lumen Only
Pittsburgh‡	143 S. 25th Street Pittsburgh, Pennsylvania, 15203, United States	Multi-tenant
Portland‡	1335 NW Northrup Street Portland, Oregon, 97209, United States	Lumen Only
Raleigh‡	5301 Departure Drive, Suite 1 Raleigh, North Carolina, 27616, United States	Multi-tenant
Reno‡	220 Gardner Street Reno, Nevada, 89503, United States	Lumen Only

Data Center	Facility Address	Occupancy
Rochester	150 Mile Crossing Boulevard Rochester, New York, 14624, United States	Lumen Only
Sacramento‡	1075 Triangle Court West Sacramento, California, 95605, United States	
Saint Louis	1015 Locust Street (3rd Floor) St. Louis, Missouri, 63101, United States	
Salt Lake City	5035 W Harold Gatty Drive Salt Lake City, Utah, 84116, United States	Multi-tenant
San Antonio‡	5130 Service Center Drive San Antonio, Texas, 78218, United States	Lumen Only
San Diego‡	8929 Aero Drive San Diego, California, 92123, United States	Multi-tenant
Santa Clara	3045 Raymond Street Santa Clara, California, 95054, United States	Lumen Only
Seattle	1000 Denny Way Seattle, Washington, 98109, United States	Multi-tenant
Southfield	19675 W. Ten Mile Road, Floors 2-3 Southfield, Michigan, 48075, United States	
Spokane	501 W 2nd Avenue Spokane, Washington, 99201, United States	Lumen Only
Stamford	21 Harborview Avenue Stamford, Connecticut, 06902, United States	Multi-tenant
Sunnyvale	1380 Kifer Road Sunnyvale, California, 94086, United States	Lumen Only
Tampa	7909 Woodland Center Boulevard Tampa, Florida, 33614, United States	
Toronto‡	8 Garamond Court Toronto, Ontario, M3C 1Z4, Canada	
Tustin‡	14452 Franklin Avenue Tustin, California, 92780, United States	
Urban Honolulu	550 Paiea Street Honolulu, Hawaii, 96819, United States	Multi-tenant
Vancouver	555 West Hastings Street, Suite 2406/1480 Vancouver, British Columbia, V6B 4N5, Canada	
Weehawken	300 Boulevard East Weehawken, New Jersey, 07086, United States	

† The noted data center facility is located within third-party data center buildings where preventative maintenance inspection activities for certain third-party-owned environmental security management systems (e.g., fire detection and suppression, cooling, backup power supply systems, etc.) are managed by and are the responsibility of the third-party building management companies. The scope of this compliance assessment only includes the preventative maintenance inspection activities for environmental management systems owned and managed by Lumen and does not include the activities performed by the third-party building management companies.

‡ Schellman applied a sampling approach to the 2022 colocation compliance assessments where a sample of 24 (of 70) sites sampled for data center visits between January 2022, and April 2022. The noted data center facilities were included in the 2022 sample selection.

Infrastructure and Software

The physical and environmental security infrastructure that supports the Lumen colocation services includes primary and secondary systems. The primary physical security systems comprise third-party commercial off-the-shelf (COTS) badge access control systems (ACS) to restrict physical access to the data center facilities and detect unauthorized access attempts for review by the PSOC. Additionally, third-party COTS closed circuit television (CCTV) video surveillance systems are in-place to record and monitor access / activity at the data center facilities. These systems are utilized to capture events and conditions related to the colocation services for review by Lumen's functional groups.

Lumen's secondary environmental security systems comprise a centralized BMS and automated ticketing system. The BMS is utilized to monitor and report on environmental conditions within the data center facilities. The BMS is integrated with the automated ticketing system and configured to notify field operations personnel, via creation of a ticket, when predefined thresholds are exceeded, such as high humidity / temperature levels on the data center floors. The automated ticketing system is also utilized for the centralized tracking of physical security events, such as the approvals for new employee badges and pre-approvals for visitors to the data center facilities. As mentioned above, the BMS and the automated ticketing system are considered secondary systems used to support the colocation services. The controls related to the maintenance and logical access to these systems are likely not relevant to the common information needs of a broad range of user entities of the colocation services. As a result, Lumen has determined the controls specific to the maintenance and logical access to the BMS, and automated ticketing system to be outside the boundaries of the system.

The in-scope infrastructure consists of the following:

Primary Infrastructure			
Production Application	**Business Function Description**	**Operating System Platform**	**Physical Location**
CCURE 9000 and Lenel	Badge access control system used to restrict physical access to the data center facilities. Reports can be generated to identify authorized badge holders as well as activity logs of successful and unsuccessful access attempts.	Windows Server 2012 R2	Local Data Centers and Broomfield, Colorado
Avigilon; Axis video encoder; Axis direct IP	Video surveillance systems used to monitor and record access and activity at the data center facilities.	Video Encoder / Appliances	Local Data Centers

People

The following are the functional areas of operations supporting the Lumen colocation:

- PSOC – provides monitoring of access controls deployed at the data center facilities including:
  - Monitoring of intrusion detection such as forced or held door alarms;
  - Analysis and response to the received alarms per incident management procedures; and
  - Assistance on alarm testing.
- Physical security (Tier 2) – supports intrusion detection sensors, video surveillance, access control systems, and applications. Team support includes, but is not limited to, repair and troubleshooting systems.
- Physical security (Tier 3) – provides advanced access control system, application, and hardware support. Oversees Tier 2 team and is the escalation point.
- Security advanced support (SAS) group for badge provisioning – oversees access control management. Customer access requests for the data center facilities are provisioned by the SAS group through assignment of access control badges. The customer designates a badge administrator who works with the SAS group to create badge accounts, update information, approve extensions, and discontinue badge access as requested.

- Field operations and data center personnel – performs facility and environmental system maintenance, provides local support for customers at the data center facility, responds to trouble and customer care tickets issued by the SAS group or BMS, and performs preventative maintenance on a scheduled basis.

Procedures

Access Provisioning and Monitoring

Logical user access requests to the badge access control and video surveillance applications are documented on a standard access request ticket and require the approval of a manager. On an annual basis, user access reviews are performed to ensure that access to the badge access control and video surveillance applications is restricted to authorized personnel. Logical access to the applications is revoked for employees as a component of the employee termination process.

Authentication and Access Control

The badge access control applications are configured to authenticate users with a user account and enforce predefined user account and minimum password requirements (e.g., password minimum length, expiration intervals, etc.). The video surveillance applications are configured to authenticate users with a unique user account and password. System authentication requirements vary from system to system. The applications utilize predefined security groups in order to assign role-based access privileges and segregate access to data. Additionally, administrative access privileges are restricted to user accounts accessible by authorized personnel. Lastly, shared user accounts within the badge access control and video surveillance applications are prohibited unless documented approval is obtained and documented via a standard exception form.

Change Management

Documented change management policies and procedures are in place to guide personnel in patch management processes. Lumen personnel implement patches to the systems hosting the in-scope COTS applications on a monthly basis in accordance with the documented procedures. Patches are applied to in-scope systems after patches are published by vendors. Additionally, Lumen personnel perform a post-implementation review of application functionality after patches have been applied to help ensure the proper functioning of the applications in the production environment. Access privileges to configure and implement patches to in-scope systems are restricted to user accounts accessible by authorized personnel.

A change management meeting is held on a weekly basis that allows for field engineering personnel to communicate ongoing and upcoming product, system, and equipment changes that may impact field operations.

Physical Security

Lumen data center facilities employ physical security controls to ensure that only authorized personnel access the data centers. Documented physical security policies and procedures are in place for employees, contractors, and visitors to address activities such as granting and revoking data center access, security monitoring, security assessments, and access activity reviews.

Each data center is equipped with badge access readers and an active, authorized badge is required for access to the data centers. The badges are used for entry and identification purposes to distinguish authorized individuals including employees, customers, contractors / vendors, and visitors (visitor badges are for identification only and do not permit data center access). The ability to create, modify, or delete badge access privileges is restricted to user accounts accessible by authorized security personnel. Additionally, video cameras are placed at entrances and exits to the data center raised floor / production areas to monitor activity. The surveillance cameras are elevated or mounted to the ceiling to prevent tampering.

Lumen PSOC personnel are staffed 24x7x365 at the corporate facilities to monitor surveillance camera feeds and badge access readers at the data centers. For ad hoc or historical review purposes, recordings from the surveillance cameras and/or badge access control system activity logs are retained for a minimum of 90 days.

Visitor (and contractor) access must be pre-approved by authorized Lumen and/or customer personnel prior to granting facility access. The access request tickets are retained by management for a minimum of 90 days, for ad hoc review by Lumen personnel. No Lumen visitors are allowed at the individual data centers that do not have a

pre-approved ticket created through the internal electronic visitation system. Upon authorization, visitors are issued a visitor badge, which is for identification purposes only and does not grant access to any of the badge readers in the data center facilities.

Persons entering the data centers must present valid government-issued photo ID, or display and use a valid Lumen-issued photo access badge, prior to being granted physical access to restricted data center areas such as the raised floor / colocation areas, equipment rooms, transport areas, and critical power and mechanical infrastructure. Visitors are required to be escorted by an authorized Lumen employee or authorized customer representative at all times while in the data centers.

The data centers located in multi-tenant facilities are monitored during business hours and access to the facilities is restricted via a badge access control system, which is separate from and does not allow access to the Lumen offices / common areas or data centers. Additional security mechanisms, such as on-site monitoring and secured fences / walls at the perimeter of the parking areas, may vary by location.

Environmental Security

Lumen has implemented and documented environmental security policies and procedures to guide personnel in equipment specifications and operating instructions, equipment inspections, and preventative maintenance schedules. Fire, heat, and smoke detectors, audible and visual alarms, water sprinklers and/or gas suppression, and hand-held fire extinguishers are installed within the data centers to protect the facilities from the threat of fire. Power management equipment, including UPS systems and/or generators, is in place to provide backup power in the event of a power outage. Redundant CRAC/HVAC units are located within the data centers to regulate temperature and humidity levels. To protect servers from water damage and to help facilitate cooling, servers are located in raised racks and water detection systems are located under the CRAC/HVAC units to detect leakage. Environmental control systems owned and managed by Lumen undergo preventive maintenance service / inspections performed by internal personnel or third-party specialists depending on the equipment type and location.

A BMS is in place and utilized to monitor environmental and availability related events for the in-scope data centers. The BMS is integrated with the ticketing system and configured to automatically generate a ticket and notify local field operations personnel when predefined thresholds are exceeded on monitored devices / equipment. Types of alerts include fire alarm status, temperature, humidity levels, and power levels.

Data Backup and Disaster Recovery

Lumen employs automated backup systems to perform scheduled backups of the production servers supporting the badge access control systems at predefined times to help ensure data center access history retention. The automated backup systems are configured to send alert notifications to IT personnel regarding backup job failures.

Lumen maintains disaster recovery plans (facility recovery and emergency management plans) for each data center facility to guide personnel in the procedures to protect against disruptions caused by an unexpected event. The facility recovery and emergency management plans are specific to each data center and include information such as plan triggers, communication plans, emergency contacts and guidelines, etc. The plans are evaluated and tested on an annual basis at each data center facility to help ensure operations can be restored in the event of a disaster.

Incident Response

Lumen has documented escalation procedures communicate employee roles and responsibilities when identifying and reporting failures, incidents, concerns, and other complaints. Incident response procedures are also in place to guide users in the incident response process and include the functional roles, processes to remediate incidents, restoration of operations, communication timelines and protocols to affected parties, and lessons learned.

An automated ticketing system is utilized to document incidents, responses, and resolution activities. To help ensure that incidents are resolved, management meets on a monthly basis to discuss and review security incidents and corrective measures.

System Monitoring

Lumen has documented policies and procedures to guide personnel in the design, development, implementation, operation, maintenance, and monitoring of in-scope systems. Lumen utilizes multiple technologies to manage and monitor security and availability risks on an ongoing basis. Lumen has implemented badge access control systems

at each in-scope data center facility to restrict and monitor activity to and within the data centers. Additionally, surveillance cameras are placed at entrances and exits to the data center raised floor / production areas to monitor activity. Lumen PSOC personnel are staffed 24x7x365 at the corporate facilities to monitor surveillance camera feeds and badge access activity at the data centers.

Lumen has also implemented various systems to monitor environmental conditions within the in-scope data centers. These systems provide real-time metrics including temperature, humidity levels, power levels, and smoke / fire detection. Environmental monitoring components feed into the Lumen BMS which is integrated with the ticketing system and configured to automatically generate a ticket and notify local field operations personnel when predefined thresholds are exceeded. In addition, customers are requested to provide feedback with respect to their own requirements related to controls and compliance.

Data

Lumen does not manage customer data / customer content being stored within Lumen's colocation services system. Physical and environmental data is managed and monitored by PSOC and field operations personnel on a 24x7x365 basis. Badge access control systems provide controlled access to the data center facilities. Video surveillance cameras are used to investigate intrusion activities or possible vulnerabilities. The badge access control systems and/or the video surveillance camera systems are configured to retain activity logs and historical recordings, respectively, for a minimum of 90 days, for ad hoc review by Lumen personnel.

The environment, including temperature and humidity, in the data center facilities is controlled using cooling systems (e.g., CRAC units, HVAC units, etc.) that are regularly maintained and inspected by third-party specialists and field services personnel. Each cooling system is attached to water leak detection sensors which are monitored 24 hours per day. The temperature and humidity levels, electrical systems, utility power, and distribution systems are monitored using the BMS. The BMS generates alarms and alert notifications for possible failure or overloading of the electrical systems.

The following table describes the information used and supported by the system.

Data Used and Supported by the System		
Data Description	**Data Reporting**	**Classification**
Badge access logs	Logged activity for the badge access system	Confidential
Security camera surveillance images	Surveillance activity pertaining to physical access to the data center facilities	

Significant Changes During the Period

There were no significant changes that are likely to affect report users' understanding of how the in-scope system is used to provide the services covered by this examination during the period.

Subservice Organizations

The environmental security management system preventative maintenance inspection services provided by third-party building management companies at the New York City (8th Ave) and Omaha data center facilities were not included within the scope of this examination.

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

Control Activity Expected to be Implemented by Subservice Organizations	Applicable Trust Services Criteria
Third-party building management companies at the New York City (8th Ave) and Omaha data center facilities are responsible for performing regular preventative maintenance inspections according to a predefined schedule for environmental control systems owned and managed by the building management companies.	A1.2

CONTROL ENVIRONMENT

The control environment at Lumen 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 executive management, the board of directors, and operations management.

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 the control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of the entity's ethical and behavioral standards, how they are communicated, and how they are reinforced in practice. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct and by example. Specific control activities that Lumen has implemented in this area include the following:

- Management formally documents the organizational policy statements that communicate Lumen's values and behavioral standards to personnel.
- Employees are required to acknowledge upon hire that they have been given access to the employee policies and procedures and understand their responsibility for adhering to them.
- Pre-hiring verification procedures are performed in accordance with regional laws and regulations for employees as a component of the hiring process.
- Employees are required to acknowledge that they have been given access to the confidentiality statement and agree not to disclose proprietary or confidential information, including client information, to unauthorized parties.
- Third parties are screened, and associated risks are evaluated by Lumen prior to onboarding.

Board of Directors and Audit Committee Oversight

The control consciousness of Lumen is influenced significantly by Lumen's board of directors and the audit committee. The board of directors meet at planned intervals and oversee operations management activities and the development and performance of internal control. During these meetings, executive management personnel discuss and monitor issues, and ensure the organization is operating in-line with Lumen's mission. Executive management is also responsible for the periodic review and approval of standards and policies to ensure that Lumen personnel are focused on achieving organizational objectives via guidance prescribed within the aforementioned

standards and policies. The independence of the board of directors is evaluated on an annual basis and results are documented and shared to external parties via their quarterly and annual financial filings. Lastly, the audit committee is in place to manage and monitor internal controls and the financial process.

Organizational Structure and Assignment of Authority and Responsibility

The Lumen organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Lumen has developed and documented policies and procedures outlining the organizational structure to communicate reporting lines and key areas of authority and responsibility, including how responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. In addition, organizational charts have been implemented to communicate key areas of authority, responsibility, and lines of reporting to personnel. These charts are communicated to employees and updated as needed.

To further define employee's responsibility within the organization and expected levels of performance, position descriptions have been documented that define the skills, responsibilities, and knowledge levels required for particular jobs.

Policies and procedures are also in place to help ensure that personnel understand Lumen's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable. Furthermore, Lumen has designated certain security and risk personnel to be aware of and manage risks as determined by the annual risk assessment.

Commitment to Competence

Lumen defines competence as the knowledge and skills necessary to accomplish tasks and define employees' roles and responsibilities. Lumen'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 Lumen has implemented in this area include the following:

- Management considers the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements.
- Pre-hiring verification procedures are performed in accordance with regional laws and regulations for employees as a component of the hiring process.
- Management conducts a performance review of employees on an annual basis to evaluate performance of employees against expected levels of performance and conduct.
- Training courses are available to new and existing employees to maintain and advance the skill level of personnel.
- Employees are required to complete security awareness training upon hire and on an annual basis thereafter to understand their obligations and responsibilities to comply with the corporate security policies.
- Management personnel monitor compliance with security awareness training requirements at least annually.

Accountability

The management philosophy and operating style at Lumen encompasses a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks; and management's attitudes toward information processing, accounting functions, and personnel. Lumen management employs a moderate risk appetite in approaching high-risk ventures. Subject matter experts are brought in early in the decision process and perform extensive due diligence. The results of those efforts are then presented to management who in turn decide whether to move forward or pass on a venture. Since the Lumen management team is hands-on and involved in the day-to-day operations of the business, executive management and operating management meet regularly to discuss the status of projects as well as review issues, risks and roadblocks related to those projects.

HR policies and practices have been developed to define the employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary processes. Management establishes accountability by setting a strong tone at the top and holding parties responsible for internal control responsibilities. Management communicates internal control responsibilities and the criteria that employees will be measured against as part of the performance review process. An employee sanction policy is also documented in the code of conduct and information security policy that address remedial actions for lack of compliance with policies and procedures.

RISK ASSESSMENT

Along with assessing risks, management has identified and put into place actions needed to address those risks. 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 mitigating identified risks and helps to ensure Lumen achieves its commitments.

Objective Setting

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

Risk Identification and Analysis

Lumen's risk identification process seeks to identify risks to the organization's ability to provide reliable services to its user entities. The organization defines risk as an uncertain event or set of events that, should they occur, will hinder the achievement of objectives. The risk assessment process begins with an asset inventory and documentation of supporting components of the asset. The risk assessment process then proceeds to determine the types of risks in place for the course of their business including data (internal and external), natural disaster, building and environmental failure, events, health and safety, physical security, people, hardware, network and software failure, and sourcing (partners and suppliers).

Risk analysis is an essential process in the organization's risk assessment process. Lumen has implemented a process whereby the threat likelihood and vulnerability of each risk is assessed and scored. A five-level scale is utilized to rate the likelihood of identified threats (a score of one is rare and a value of five is almost certain); the likelihood score utilizes multiple factors when determining the score, including: statistics (when available), experience for natural and technical threats, and investment and level of expertise required for intentional threats. After the likelihood of a threat has been determined, the potential impact of the threat is defined by the asset owner. The impact is also rated on a five-level scale (a score of one being insignificant and five being catastrophic).

Once the likelihood and impact values have been determined, the initial risk rating is calculated by combining the two values as depicted in the following table:

	Consequence				
Likelihood	**1**	**2**	**3**	**4**	**5**
5 – Almost Certain	Medium	High	High	Extreme	Extreme
4 - Likely	Medium	Medium	High	High	Extreme

Consequence					
Likelihood	**1**	**2**	**3**	**4**	**5**
3 - Possible	Low	Medium	High	High	High
2 - Unlikely	Low	Low	Medium	Medium	High
1 - Rare	Low	Low	Medium	Medium	High

Mitigating controls are considered and applied to the initial risk rating score to determine the residual risk rating. There are four categories of mitigating controls considered by the asset owner during the risk analysis process as defined in the below table:

Categories	Vulnerability
Physical	Physical mechanisms that directly limit or control access to information like gates or barricades, security guards, locked doors, locked filing cabinets, and Lenel controlled doors.
Electronic or Technical	Virtual and technical controls (systems and software) that electronically limit or control information access, such as card reader systems (card readers, badges, and monitoring system), building management system, video surveillance (CCTV, recorders, displays), firewalls, anti-virus software, encryption, etc.
Access	Mechanisms to limit or control information access based on user authorization, identification and authentication, access approval, accountability, RSA Tokens, role-based access control, etc.
Administrative	Mechanisms that limit or control information access based on the performance or management of business operations through policies, work instructions, written procedures, or rules.

The final residual risk rating is what determines the risk treatment is based on Lumen's risk appetite, which determines how much risk the business is willing to accept before mitigation controls are implemented. A four-level scale is utilized to guide the risk treatment strategy as represented in the following table:

Level	Risk Treatment Strategy
Low	· Maintain current actions, resources, and strategies to prevent the escalation of the risk · Risk treatment is not required
Medium	· Take actions to reduce where benefit exceeds cost and/or continue to implement actions · Risk treatment may be required
High	· Existing actions, resources or strategies must be modified as soon as possible · Risk treatment required
Extreme	· Improved actions, resources and strategies are required to be implemented immediately · Risk treatment required

If the residual risk rating is of a level that requires action, additional controls will be implemented using a risk treatment plan. Asset owners and the compliance group work together to implement risk treatments. If management does not accept the residual risk level, then additional controls will be implemented to further reduce the risk.

The register also provides a snapshot of the identified risks for the organizational activity in question, the priority of each of the risks, the risk owner and the response strategy chosen by each risk owner, the risk closure time and rationalization.

Risk Factors

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

External Factors

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

Internal Factors

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

Potential for Fraud

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

Management realizes that the potential for fraud can occur when employees are motivated by certain pressures or incentivized to commit fraud. The absence of controls, or ineffective controls, provides an opportunity for fraud when combined with an incentive to commit fraud. Therefore, the risk assessment that is performed on an annual basis, considers the potential for fraud.

Risk Mitigation

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

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

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

TRUST SERVICES CRITERIA AND RELATED CONTROL ACTIVITIES

Integration with Risk Assessment

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

Selection and Development of Control Activities

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

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

Trust Services Criteria Not Applicable to the In-Scope System

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

INFORMATION AND COMMUNICATION SYSTEMS

Pertinent information must be identified, captured, and communicated in a form and timeframe that enables personnel to carry out their responsibilities. Information systems produce reports, containing operational, financial, and compliance-related information, that make it possible to run and control the business. They deal not only with internally generated data, but also information about external events, activities, and conditions necessary to inform business decision-making and external reporting. Effective communication also must occur in a broader sense, flowing down, across and up the organization. Personnel receive a clear message from top management that control responsibilities must be taken seriously. They must understand their own role in the internal control system, as well as how individual activities relate to the work of others. They must have a means of communicating significant information upstream. There also needs to be effective communication with external parties, such as customers, suppliers, regulators, and shareholders.

Internal Communications

Information is necessary for Lumen to carry out internal control responsibilities to support the achievement of its objectives related to the colocation services system. Lumen has implemented various methods of communication to help provide assurance that employees understand their individual roles and responsibilities and that significant events are communicated. These methods include orientation for new employees, training for employees, and the use of e-mail messages and internal communications tools to communicate time-sensitive information.

Employees are required to complete security awareness training upon hire and on an annual basis thereafter to understand their obligations and responsibilities in complying with the corporate security policies. A training portal is also available to employees to help maintain and advance their skillset and certifications, as applicable. Employees are required to acknowledge the code of conduct upon hire indicating that they have been given access to the code of conduct and understand their responsibility for reporting internal incidents, concerns, and complaints.

Lumen's code of conduct also informs the employee of what the company deems confidential information and the employee's role in making sure any confidential information stored, handled, received, or processed appropriately.

Policies and procedures are in place to guide personnel in the design, development, implementation, operation, maintenance, and monitoring of in-scope systems. Escalation procedures for reporting security incidents are in place to guide personnel in identifying and reporting failures, incidents, concerns, and other complaints. These policies and procedures are communicated to internal personnel via the company intranet. A ticketing system is utilized to document security incidents and employees can submit anonymous incidents, concerns, and complaints to the Lumen Integrity Line via e-mail, phone call or the public-facing website. Additionally, engineering department meetings are held on a weekly basis to communicate departmental performance and address operational problems.

External Communications

Lumen has also implemented various methods of communication to help provide assurance that customers understand the roles and responsibilities in the communication of significant events. Customer support and incident reporting methods are documented and communicated to customers for submitting support requests and reporting incidents. These methods include the use of e-mail, live chat sessions, and phone support accessible within Control Center. Additionally, external parties and customers can submit anonymous incidents, concerns, and complaints to Lumen via e-mail or the public-facing website. Information regarding the design and operation of the system and its boundaries is communicated via the company website, service level agreements, and service guides; commitments made by Lumen are communicated via the service level agreements and service guides. The security and availability commitments and obligations of suppliers are documented and communicated via the supplier code of conduct.

MONITORING

Monitoring is a process that assesses the quality of internal control performance over time. It involves assessing the design and operation of controls and taking necessary corrective actions. This process is accomplished through ongoing activities, separate evaluation, or a combination of the two.

Ongoing Monitoring

Lumen performs ongoing monitoring to help ensure that business systems operate effectively on a continuous basis. Aspects of the ongoing monitoring procedures include the following:

- The audit committee establishes and maintains a formal audit committee charter that describes their roles and responsibilities. The charter is available via the customer-facing website.
- Physical security and availability monitoring systems (e.g., security alarms, surveillance cameras, BMS, etc.) are utilized to monitor and analyze the in-scope systems for possible or actual security breaches and system availability incidents.
- Data center security personnel and the PSOC monitor access to the data centers 24 hours a day, seven days a week, using reports from the physical security access mechanisms, alarms, and CCTV video surveillance systems.

Separate Evaluations

Lumen has placed a greater degree of reliance of ongoing monitoring activities resulting in a reduced need for separate evaluations; however, management has still implemented evaluation activities that include the review of system and organization control audits and ISO certifications performed by third parties and vendor analysis activities. Management evaluates the performance of specific control activities based on the results of these evaluation activities and the results are reviewed by management to determine the effectiveness of Lumen's control activities. As a result of management's risk analysis process, each control activity within scope is assigned a risk level associated with the risk it is intended to mitigate (as documented and tracked within the risk register). Controls that serve to mitigate multiple risks are assigned the highest level of assessed risk among the pertinent risks.

Monitoring of Subservice Organizations

A vendor management policy is in place to guide personnel in the periodic evaluation and monitoring of risks arising from the use of vendors. As part of the vendor selection and onboarding process, Lumen personnel perform a risk assessment that results in a cumulative risk level. The assessed risk level determines the periodicity with which periodic audit reviews are to take place.

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

Evaluating and Communicating Deficiencies

Deviations or deficiencies identified as part of the ongoing and scheduled monitoring activities that are associated with controls with a high-risk level assignment are escalated to management for immediate corrective action. Management reviews the deviations and corrective actions during the annual risk assessment.

COMPLEMENTARY CONTROLS AT USER ENTITIES

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

SECTION 4

TESTING MATRICES

TESTS OF OPERATING EFFECTIVENESS AND RESULTS OF TESTS

Scope of Testing

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

Tests of Operating Effectiveness

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

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

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

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

Sampling

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

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

Reliability of Information Provided by the Service Organization

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

Test Results

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

SECURITY CATEGORY

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
Control Environment			
CC1.1 COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
CC1.1.1	Management formally documents the organizational policy statements that communicate Lumen's values and behavioral standards to personnel.	Inspected the code of conduct and employee handbook to determine that management formally documented and reviewed the organizational policy statements that communicated Lumen's values and behavioral standards to personnel on an annual basis.	No exceptions noted.
CC1.1.2	Employees are required to acknowledge upon hire that they have been given access to the employee policies and procedures and understand their responsibility for adhering to them.	Inspected the code of conduct acknowledgment for a sample of employees hired during the period to determine that each employee sampled acknowledged that they had been given access to the employee policies and procedures and understood their responsibility for adhering to them.	No exceptions noted.
CC1.1.3	Pre-hiring verification procedures are performed in accordance with regional laws and regulations for employees as a component of the hiring process.	Inspected the background check guidelines to determine that a policy was in place to guide personnel in performing pre-hiring verification procedures.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the completed background check for a sample of employees hired during the period to determine that pre-hiring verification procedures were performed in accordance with regional laws and regulations for each employee sampled.	No exceptions noted.
CC1.1.4	Employees are required to acknowledge that they have been given access to the confidentiality statement and agree not to disclose proprietary or confidential information, including client information, to unauthorized parties.	Inspected the accepted offer letter for a sample of employees hired during the period to determine that each employee sampled acknowledged that they were given access to the confidentiality statement and agreed not to disclose proprietary or confidential information, including client information, to unauthorized parties.	No exceptions noted.
CC1.1.5	Third parties are screened, and associated risks are evaluated by Lumen prior to onboarding.	Observed the company website and prospective supplier registration form with the assistance of the senior information security auditor to determine that third parties were screened, and associated risks were evaluated by Lumen prior to onboarding.	No exceptions noted.
		Inspected the vendor management procedures to determine that third parties were screened, and associated risks were evaluated by Lumen prior to onboarding.	No exceptions noted.
CC1.2 COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
CC1.2.1	A formal charter and set of bylaws is documented that describes the responsibilities of the board of directors regarding oversight of management's system of internal control.	Inspected the charter and bylaws to determine that a formal charter and set of bylaws was documented that described the responsibilities of the board of directors regarding oversight of management's system of internal control.	No exceptions noted.
CC1.2.2	The board of directors, with the assistance of the nominating and corporate governance committee, evaluates the independence of its members on an annual basis to ensure that a majority of its members are independent from management.	Inspected Lumen's most recent proxy report to determine that the board of directors, with the assistance of the nominating and corporate governance committee, evaluated the independence of its members during the period to ensure that a majority of its members were independent from management.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.3 COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
CC1.3.1	Management formally documents the organizational policy statements that communicate Lumen's values and behavioral standards to personnel.	Inspected the code of conduct and employee handbook to determine that management formally documented and reviewed the organizational policy statements that communicated Lumen's values and behavioral standards to personnel on an annual basis.	No exceptions noted.
CC1.3.2	The organizational structure, reporting lines, and authorities are defined in organizational charts, updated on an as-needed basis, and communicated to employees.	Inquired of the senior information security auditor regarding organizational management to determine that the organizational structure, reporting lines, and authorities were updated on an as-needed basis.	No exceptions noted.
		Inspected the organizational charts displayed on the company intranet to determine that the organizational structure, reporting lines, and authorities were defined and communicated to employees.	No exceptions noted.
CC1.3.3	Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements.	Inspected the written position requirements for a sample of employees hired during the period to determine that management considered the competence levels for each employee sampled and translated required skills and knowledge levels into written position requirements.	No exceptions noted.
CC1.3.4	Security and risk personnel are responsible for managing security and availability risks.	Inspected the information security policy to determine that security and risk personnel were responsible for managing security and availability risks.	No exceptions noted.
CC1.4 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC1.4.1	Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements.	Inspected the written position requirements for a sample of employees hired during the period to determine that management considered the competence levels for each employee sampled and translated required skills and knowledge levels into written position requirements.	No exceptions noted.
CC1.4.2	Pre-hiring verification procedures are performed in accordance with regional laws and regulations for employees as a component of the hiring process.	Inspected the background check guidelines to determine that a policy was in place to guide personnel in performing pre-hiring verification procedures.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the completed background check for a sample of employees hired during the period to determine that pre-hiring verification procedures were performed in accordance with regional laws and regulations for each employee sampled.	No exceptions noted.
CC1.4.3	Management conducts a performance review of employees on an annual basis to evaluate performance of employees against expected levels of performance and conduct.	Inspected the completed performance review for a sample of current employees to determine that management conducted a performance review during the period for each sampled employee to evaluate their performance against expected levels of performance and conduct.	No exceptions noted.
CC1.4.4	Training courses are available to new and existing employees to maintain and advance the skill level of personnel.	Inspected the list of training courses available on the company learning center to determine that training courses were available to new and existing employees to maintain and advance the skill level of personnel.	No exceptions noted.
CC1.4.5	Employees are required to complete security awareness training upon hire and on an annual basis thereafter to understand their obligations and responsibilities to comply with the corporate security policies.	Inquired of the senior information security auditor regarding security awareness training to determine that employees were required to complete security awareness training upon hire and on an annual basis thereafter to understand their obligations and responsibilities to comply with the corporate security policies.	No exceptions noted.
		Inspected the security awareness training results for a sample of current employees to determine that each employee sampled completed security awareness training during the period.	No exceptions noted.
		Inspected the security awareness training results for a sample of employees hired during the period to determine that each employee sampled completed security awareness training upon hire.	No exceptions noted.
CC1.4.6	Management personnel monitor compliance with security awareness training requirements at least annually.	Inspected an example notification from the training department received during the period to determine that management personnel monitored compliance with security awareness training requirements at least annually.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.5 COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CC1.5.1	Management formally documents the organizational policy statements that communicate Lumen's values and behavioral standards to personnel.	Inspected the code of conduct and employee handbook to determine that management formally documented and reviewed the organizational policy statements that communicated Lumen's values and behavioral standards to personnel on an annual basis.	No exceptions noted.
CC1.5.2	Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements.	Inspected the written position requirements for a sample of employees hired during the period to determine that management considered the competence levels for each employee sampled and translated required skills and knowledge levels into written position requirements.	No exceptions noted.
CC1.5.3	Management conducts a performance review of employees on an annual basis to evaluate performance of employees against expected levels of performance and conduct.	Inspected the completed performance review for a sample of current employees to determine that management conducted a performance review during the period for each sampled employee to evaluate their performance against expected levels of performance and conduct.	No exceptions noted.
CC1.5.4	An employee sanction policy is in place that address remedial actions for lack of compliance with policies and procedures.	Inspected the employee code of conduct policy and information security policy to determine that an employee sanction policy was in place that addressed remedial actions for lack of compliance with policies and procedures.	No exceptions noted.
Communication and Information			
CC2.1 COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
CC2.1.1	Documented policies and procedures are in place that identify information required to support the functioning of internal control and achievement of objectives and associated protection, access rights, and retention requirements.	Inspected the corporate security policies and procedures to determine that documented policies and procedures were in place that identified information required to support the functioning of internal control and achievement of objectives and associated protection, access rights, and retention requirements.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.1.2	Lumen's IT security group monitors the security impact of emerging technologies, and the impact of applicable laws or regulations are considered by senior management.	Inspected example security updates and notifications received during the period to determine that Lumen's IT security group monitored the security impact of emerging technologies, and the impact of applicable laws or regulations were considered by senior management.	No exceptions noted.
CC2.1.3	Physical security and availability monitoring applications are utilized to monitor and analyze the in-scope systems for possible or actual security breaches and system availability incidents.	Inspected the security and availability monitoring application configurations to determine that physical security and availability monitoring applications were utilized to monitor and analyze the in-scope systems for possible or actual security breaches and system availability incidents.	No exceptions noted.
CC2.1.4	A ticketing system is in place to allow customers to submit support requests and report incidents.	Inspected the customer support portal and new repair ticket form to determine that a ticketing system was in place to allow customers to submit support requests and report incidents.	No exceptions noted.
CC2.2 COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
CC2.2.1	Documented policies and procedures are in place to guide personnel in the design, development, implementation, operation, maintenance, and monitoring of in-scope systems.	Inspected the corporate security policies and procedures to determine that documented policies and procedures were in place to guide personnel in the design, development, implementation, operation, maintenance, and monitoring of in-scope systems.	No exceptions noted.
CC2.2.2	Employees are required to complete security awareness training upon hire and on an annual basis thereafter to understand their obligations and responsibilities to comply with the corporate security policies.	Inquired of the senior information security auditor regarding security awareness training to determine that employees were required to complete security awareness training upon hire and on an annual basis thereafter to understand their obligations and responsibilities to comply with the corporate security policies.	No exceptions noted.
		Inspected the security awareness training results for a sample of current employees to determine that each employee sampled completed security awareness training during the period.	No exceptions noted.
		Inspected the security awareness training results for a sample of employees hired during the period to determine that each employee sampled completed security awareness training upon hire.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.2.3	Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements.	Inspected the written position requirements for a sample of employees hired during the period to determine that management considered the competence levels for each employee sampled and translated required skills and knowledge levels into written position requirements.	No exceptions noted.
CC2.2.4	Employees are required to acknowledge upon hire that they have been given access to the employee policies and procedures and understand their responsibility for adhering to them.	Inspected the code of conduct acknowledgment for a sample of employees hired during the period to determine that each employee sampled acknowledged that they had been given access to the employee policies and procedures and understood their responsibility for adhering to them.	No exceptions noted.
CC2.2.5	Training courses are available to new and existing employees to maintain and advance the skill level of personnel.	Inspected the list of training courses available on the company learning center to determine that training courses were available to new and existing employees to maintain and advance the skill level of personnel.	No exceptions noted.
CC2.2.6	Documented escalation procedures for security and availability incidents are provided to internal users to guide users in identifying and reporting failures, incidents, concerns, and other complaints.	Inspected the incident response and escalation procedures to determine that documented escalation procedures for reporting security and availability incidents were provided to internal users to guide users in identifying and reporting failures, incidents, concerns, and other complaints.	No exceptions noted.
CC2.2.7	An automated ticketing system is utilized to document security and availability incidents, responses, and resolution activities.	Inspected the automated incident ticket generation configurations to determine that an automated ticketing system was utilized to document security and availability incidents, responses, and resolution activities.	No exceptions noted.
CC2.2.8	An online whistleblower channel is accessible by internal users to report incidents, concerns, and complaints.	Inspected the Lumen intranet to determine that an online whistleblower channel was accessible by internal users to report incidents, corrections, and complaints.	No exceptions noted.
CC2.2.9	Management conducts a performance review of employees on an annual basis to evaluate performance of employees against expected levels of performance and conduct.	Inspected the completed performance review for a sample of current employees to determine that management conducted a performance review during the period for each sampled employee to evaluate their performance against expected levels of performance and conduct.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.3 COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
CC2.3.1	Information regarding the design and operation of the system and its boundaries is communicated to external users via the company website, customer contracts, and service guides.	Inspected the data center user guide and the customer contract template to determine that information regarding the design and operation of the system and its boundaries were communicated to external users via the company website, customer contracts, and service guides.	No exceptions noted.
CC2.3.2	Lumen's security and availability commitments and the associated system requirements are documented and communicated to internal and external users via the standard SLA, data center user guide, and customer contracts.	Inspected the standard SLA, data center user guide, and customer contract to determine that Lumen's security and availability commitments and the associated system requirements were documented and communicated to internal and external users.	No exceptions noted.
CC2.3.3	The security commitments and obligations of suppliers are documented and communicated via the supplier code of conduct.	Inspected the supplier code of conduct to determine that the security commitments and obligations of suppliers were documented and communicated via the supplier code of conduct.	No exceptions noted.
CC2.3.4	An online whistleblower channel is accessible by external users to report incidents, concerns, and complaints.	Inspected the public-facing website to determine that an online whistleblower channel was accessible by external users to report incidents, corrections, and complaints.	No exceptions noted.
CC2.3.5	A ticketing system is in place to allow customers to submit support requests and report incidents.	Inspected the customer support portal and new repair ticket form to determine that a ticketing system was in place to allow customers to submit support requests and report incidents.	No exceptions noted.
Risk Assessment			
CC3.1 COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
CC3.1.1	Documented policies and procedures are in place to guide personnel in performing the annual risk assessment that include the risk scoring methodology, risk tolerance levels, and the development of risk treatment plans to mitigate risk.	Inspected the risk assessment policies and procedures and most recent risk assessment to determine that policies and procedures were in place to guide personnel in performing the annual risk assessment that included the risk scoring methodology, risk tolerance levels, and the development of risk treatment plans to mitigate risk.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.1.2	Lumen's security and compliance objectives are documented within the information security policy. The information security policy is reviewed and approved by management on an annual basis.	Inspected the information security policy to determine that Lumen's security and compliance objectives were documented, and the information security policy was reviewed and approved by management during the period.	No exceptions noted.
CC3.1.3	A risk assessment is performed on an annual basis that considers the identification and assessment of risk related to the documented objectives and changes that could significantly impact the system. Identified risks are rated using a risk evaluation process and are formally documented, with mitigation strategies, for management review.	Inspected the most recent risk assessment to determine that a risk assessment was performed during the period that considered the identification and assessment of risks relating to the documented objectives and changes that could significantly impact the system and that identified risks were rated using a risk evaluation process and were formally documented, with mitigation strategies, for management review.	No exceptions noted.
CC3.2 COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
CC3.2.1	Documented policies and procedures are in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk mitigation strategies as a part of the risk assessment process.	Inspected the risk management policies and procedures to determine that policies and procedures were in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk mitigation strategies as a part of the risk assessment process.	No exceptions noted.
CC3.2.2	A listing of assets and locations within the scope of services is maintained and reviewed as part of the annual risk assessment process.	Inspected the asset inventory listing and most recent risk assessment to determine that a listing of assets and locations within the scope of services was maintained and reviewed as part of the annual risk assessment process.	No exceptions noted.
CC3.2.3	A risk assessment is performed at least annually that considers the identification and assessment of risk related to the documented objectives and changes that could significantly impact the system. Identified risks are rated using a risk evaluation process and are formally documented, with mitigation strategies, for management review.	Inspected the most recent risk assessment to determine that a risk assessment was performed during the period that considered the identification and assessment of risks relating to the documented objectives and changes that could significantly impact the system and that identified risks were rated using a risk evaluation process and were formally documented, with mitigation strategies, for management review.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.2.4	Lumen's IT security group monitors the security impact of emerging technologies, and the impact of applicable laws or regulations are considered by senior management.	Inspected example security updates and notifications received during the period to determine that Lumen's IT security group monitored the security impact of emerging technologies, and the impact of applicable laws or regulations were considered by senior management.	No exceptions noted.
CC3.2.5	Risks arising from the use of vendors providing goods and services are analyzed as part of the annual risk assessment.	Inspected the most recent risk assessment and review of vendors security assessment to determine that risks arising from the use of vendors providing goods and services were analyzed as part of the annual risk assessment.	No exceptions noted.
CC3.3 COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
CC3.3.1	Documented policies and procedures are in place to guide personnel in identifying the potential for fraud when performing the risk assessment process.	Inspected the risk assessment policies and procedures to determine that documented policies and procedures were in place to guide personnel in identifying the potential for fraud when performing the risk assessment process.	No exceptions noted.
CC3.3.2	A risk assessment is performed at least annually that considers the potential for fraud. Identified risks are rated using a risk evaluation process and are formally documented, with mitigation strategies, for management review.	Inspected the most recent risk assessment to determine that a risk assessment was performed during the period that considered the potential for fraud and that identified risks were rated using a risk evaluation process and were formally documented, with mitigation strategies, for management review.	No exceptions noted.
CC3.4 COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
CC3.4.1	A risk assessment is performed at least annually that considers the identification and assessment of risk related to the documented objectives and changes that could significantly impact the system. Identified risks are rated using a risk evaluation process and are formally documented, with mitigation strategies, for management review.	Inspected the most recent risk assessment to determine that a risk assessment was performed during the period that considered the identification and assessment of risks relating to the documented objectives and changes that could significantly impact the system and that identified risks were rated using a risk evaluation process and were formally documented, with mitigation strategies, for management review.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.4.2	Developments in technology and the impact of applicable laws or regulations are considered by senior management as part of monthly compliance and legal review meetings.	Inspected the compliance and legal review meeting minutes for a sample of months during the period to determine that developments in technology and the impact of applicable laws or regulations were considered by senior management as part of monthly compliance and legal review meetings for each month sampled.	No exceptions noted.
CC3.4.3	Lumen's IT security group monitors the security impact of emerging technologies, and the impact of applicable laws or regulations are considered by senior management.	Inspected example security updates and notifications received during the period to determine that Lumen's IT security group monitored the security impact of emerging technologies, and the impact of applicable laws or regulations were considered by senior management.	No exceptions noted.
Monitoring Activities			
CC4.1 COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
CC4.1.1	Surveillance cameras are utilized to monitor access to the office buildings and data centers and are located at entrances and exits to the data center raised floor / production areas.	Inquired of the security compliance auditor regarding facility monitoring to determine that surveillance cameras were utilized to monitor access to the office buildings and data centers and were located at entrances and exits to the data center raised floor / production areas.	No exceptions noted.
		Observed the presence of surveillance cameras for a sample of in-scope data center facilities to determine that surveillance cameras were utilized to monitor access to the office buildings and data centers and were located at entrances and exits to the data center raised floor / production areas.	No exceptions noted.
		Inspected the surveillance camera placement maps for a sample of in-scope data center facilities to determine that surveillance cameras were in place to monitor access to the office buildings and data centers and were located at entrances and exits to the data center raised floor / production areas.	The test of the control activity disclosed that a surveillance camera placement map was not in place for the following one (1) of 24 data center facilities sampled: Newark

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC4.1.2	Data center security personnel and the PSOC monitor access to the data centers 24 hours a day, seven days a week, using reports from the physical security access mechanisms, alarms, and CCTV video surveillance systems.	Inquired of the security compliance auditor regarding facility monitoring to determine that data center security personnel and the PSOC monitored access to the data centers 24 hours a day, seven days a week, using reports from the physical security access mechanisms, alarms, and CCTV video surveillance systems.	No exceptions noted.
		Inspected the PSOC staffing schedules during the period to determine that PSOC personnel were staffed 24 hours per day, seven days per week.	No exceptions noted.
CC4.1.3	A BMS is configured to monitor data center equipment including, but not limited to, the following: · Fire alarm status and suppression systems · Temperature and humidity levels · Power levels and availability	Inspected the BMS configurations to determine that a BMS was utilized to monitor data center equipment including, but not limited to, the following: · Fire alarm status and suppression systems · Temperature and humidity levels · Power levels and availability	No exceptions noted.
CC4.1.4	The BMS is integrated with the ticketing system and configured to generate a ticket and alert local field operations personnel when predefined thresholds are exceeded on monitored devices.	Inspected the BMS configurations and an example alert generated during the period to determine that a BMS was integrated with the ticketing system and configured to generate a ticket and alert local field operations personnel when predefined thresholds were exceeded on monitored devices.	No exceptions noted.
CC4.2 COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.			
CC4.2.1	Documented escalation procedures for security and availability incidents are provided to internal users to guide users in identifying and reporting failures, incidents, concerns, and other complaints.	Inspected the incident response and escalation procedures to determine that documented escalation procedures for reporting security and availability incidents were provided to internal users to guide users in identifying and reporting failures, incidents, concerns, and other complaints.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC4.2.2	Data center security personnel and the PSOC monitor access to the data centers 24 hours a day, seven days a week, using reports from the physical security access mechanisms, alarms, and CCTV video surveillance systems.	Inquired of the security compliance auditor regarding facility monitoring to determine that data center security personnel and the PSOC monitored access to the data centers 24 hours a day, seven days a week, using reports from the physical security access mechanisms, alarms, and CCTV video surveillance systems.	No exceptions noted.
		Inspected the PSOC staffing schedules during the period to determine that PSOC personnel were staffed 24 hours per day, seven days per week.	No exceptions noted.
CC4.2.3	The BMS is integrated with the ticketing system and configured to generate a ticket and alert local field operations personnel when predefined thresholds are exceeded on monitored devices.	Inspected the BMS configurations and an example alert generated during the period to determine that a BMS was integrated with the ticketing system and configured to generate a ticket and alert local field operations personnel when predefined thresholds were exceeded on monitored devices.	No exceptions noted.
CC4.2.4	Management meetings are held on a monthly basis to discuss security incidents and corrective measures to help ensure that incidents are resolved.	Inspected the management meeting minutes for a sample of months during the period to determine that management meetings were held to discuss security incidents and corrective measures to help ensure incidents were resolved for each month sampled.	No exceptions noted.
CC4.2.5	Management meetings are held on a monthly basis to review availability trends and availability forecasts as compared to system commitments.	Inspected the management meeting minutes for a sample of months during the period to determine that management meetings were held each month sampled to review availability trends and forecasts as compared to system commitments.	No exceptions noted.
Control Activities			
CC5.1 COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			
CC5.1.1	Documented policies and procedures are in place to guide personnel in performing the annual risk assessment that include the risk scoring methodology, risk tolerance levels, and the development of risk treatment plans to mitigate risk.	Inspected the risk assessment policies and procedures and most recent risk assessment to determine that policies and procedures were in place to guide personnel in performing the annual risk assessment that included the risk scoring methodology, risk tolerance levels, and the development of risk treatment plans to mitigate risk.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.1.2	A 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.	Inspected the most recent risk assessment documentation to determine that a formal risk assessment was performed during the period and that identified risks were formally documented for management review.	No exceptions noted.
CC5.1.3	Assigned risk owners select and develop control activities to mitigate the risks identified during the annual risk assessment process. The control activities are documented within risk treatment plans that are created by the risk owners for risks above the tolerable threshold.	Inspected the most recent risk assessment to determine that assigned risk owners selected and developed control activities to mitigate the risks identified during the annual risk assessment process and that control activities were documented within risk treatment plans that were created by the risk owners for risks above the tolerable threshold.	No exceptions noted.
CC5.2 COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
CC5.2.1	Assigned risk owners select and develop control activities over technology to support the achievement of objectives as an output from the risk assessment performed on an annual basis. The control activities are documented within the mitigation plans that are created by the risk owners for risks above the tolerable threshold.	Inspected the most recent risk assessment to determine that assigned risk owners selected and developed control activities over technology to support the achievement of objectives as an output from the risk assessment performed on an annual basis and that control activities were documented within the mitigation plans created by the risk owners for risks above the tolerable threshold.	No exceptions noted.
CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC5.3.1	Documented policies and procedures are in place to guide personnel in the design, development, implementation, operation, maintenance, and monitoring of in-scope systems.	Inspected the corporate security policies and procedures to determine that documented policies and procedures were in place to guide personnel in the design, development, implementation, operation, maintenance, and monitoring of in-scope systems.	No exceptions noted.
CC5.3.2	Documented policies and procedures are in place that identify information required to support the functioning of internal control and achievement of objectives and associated protection, access rights, and retention requirements.	Inspected the corporate security policies and procedures to determine that documented policies and procedures were in place that identified information required to support the functioning of internal control and achievement of objectives and associated protection, access rights, and retention requirements.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.3.3	Employees are required to acknowledge upon hire that they have been given access to the employee policies and procedures and understand their responsibility for adhering to them.	Inspected the code of conduct acknowledgment for a sample of employees hired during the period to determine that each employee sampled acknowledged that they had been given access to the employee policies and procedures and understood their responsibility for adhering to them.	No exceptions noted.
CC5.3.4	An employee sanction policy is in place that address remedial actions for lack of compliance with policies and procedures.	Inspected the employee code of conduct policy and information security policy to determine that an employee sanction policy was in place that addressed remedial actions for lack of compliance with policies and procedures.	No exceptions noted.
Logical and Physical Access Controls			
CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
CC6.1.1	Documented policies and procedures are in place to guide personnel in the acceptable use of information assets.	Inspected the information security policy and the code of conduct to determine that documented policies and procedures were in place to guide personnel in the acceptable use of information assets.	No exceptions noted.
CC6.1.2	Badge access control applications are configured to authenticate users with a user account and password. The badge access control applications are configured to enforce the following password requirements: · Password minimum length · Password expiration intervals · Password complexity requirements · Password minimum history · Invalid password account lockout threshold	Inquired of the senior information security auditor regarding badge access control application authentication configurations to determine that badge access control applications were configured to authenticate users with a user account and password and were configured to enforce the following password requirements: · Password minimum length · Password expiration intervals · Password complexity requirements · Password minimum history · Invalid password account lockout threshold	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the user account listings and minimum password requirements for the badge access systems to determine that badge access control applications were configured to authenticate users with a user account and password and were configured to enforce the following password requirements: · Password minimum length · Password expiration intervals · Password complexity requirements · Password minimum history · Invalid password account lockout threshold	No exceptions noted.
CC6.1.3	Video surveillance applications are configured to authenticate users with a user account and password.	Inspected the user account listings and authentication configurations for the in-scope video surveillance applications to determine that the video surveillance applications were configured to authenticate users with a user account and password.	No exceptions noted.
CC6.1.4	Predefined security groups are utilized to assign role-based access privileges and segregate access to data within the badge access control and video surveillance applications.	Inspected the user account listings for the in-scope badge access and video surveillance applications to determine that predefined security groups were utilized to assign role-based access privileges and segregate access to data.	No exceptions noted.
CC6.1.5	Shared user accounts within the badge access control and video surveillance applications are prohibited unless documented approval is obtained and documented via a standard exception form.	Inquired of the senior information security auditor regarding shared user accounts to determine that shared user accounts within the badge access control and video surveillance applications were prohibited unless documented approval was obtained and documented via a standard exception form.	No exceptions noted.
		Inspected the standard exception form for a sample of shared user accounts within the badge access control and video surveillance applications to determine that each shared user account sampled had an approved standard exception form.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.1.6	Administrative access privileges within the badge access control and video surveillance applications are restricted to user accounts accessible by authorized security personnel.	Inspected the administrator user account listings for the in-scope badge access control and video surveillance applications with the assistance of the senior information security auditor to determine that administrative access privileges were restricted to user accounts accessible by authorized security personnel.	No exceptions noted.
CC6.1.7	The ability to create, modify, or remove badge access users and privileges is restricted to administrator user accounts accessible by authorized security personnel.	Inspected the badge access control system administrator user account listing with the assistance of the senior information security auditor to determine that the ability to create, modify, or remove badge access privileges was restricted to administrator user accounts accessible by authorized security personnel.	No exceptions noted.
CC6.1.8	A listing of assets and locations within the scope of services is maintained and reviewed as part of the annual risk assessment process.	Inspected the asset inventory listing and most recent risk assessment to determine that a listing of assets and locations within the scope of services was maintained and reviewed as part of the annual risk assessment process.	No exceptions noted.
CC6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			
CC6.2.1	Logical user access requests to the badge access control and video surveillance applications are documented on a standard access request ticket and require the approval of a manager.	Inspected the access request ticket for a sample of accounts provisioned during the period to determine that logical user access requests to the badge access control and video surveillance applications were documented on a standard access request ticket and required the approval of a manager for each sampled access request.	No exceptions noted.
CC6.2.2	Logical access to the badge access control and video surveillance applications is revoked for employees as a component of the employee termination process.	Inspected the user account listings for the in-scope badge access control and video surveillance applications for a sample of employees terminated during the period to determine that logical access to the badge access control and video surveillance systems was revoked for each terminated employee sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.2.3	Logical user access reviews are performed on an annual basis to help ensure that access to the badge access control and video surveillance applications is restricted.	Inspected the most recently completed logical user access review for the in-scope badge access control and video surveillance applications to determine that an access review was performed during the period.	No exceptions noted.
CC6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.			
CC6.3.1	Logical user access requests to the badge access control and video surveillance applications are documented on a standard access request ticket and require the approval of a manager.	Inspected the access request ticket for a sample of accounts provisioned during the period to determine that logical user access requests to the badge access control and video surveillance applications were documented on a standard access request ticket and required the approval of a manager for each sampled access request.	No exceptions noted.
CC6.3.2	Logical access to the badge access control and video surveillance applications is revoked for employees as a component of the employee termination process.	Inspected the user account listings for the in-scope badge access control and video surveillance applications for a sample of employees terminated during the period to determine that logical access to the badge access control and video surveillance systems was revoked for each terminated employee sampled.	No exceptions noted.
CC6.3.3	Predefined security groups are utilized to assign role-based access privileges and segregate access to data within the badge access control and video surveillance applications.	Inspected the user account listings for the in-scope badge access and video surveillance applications to determine that predefined security groups were utilized to assign role-based access privileges and segregate access to data.	No exceptions noted.
CC6.3.4	Shared user accounts within the badge access control and video surveillance applications are prohibited unless documented approval is obtained and documented via a standard exception form.	Inquired of the senior information security auditor regarding shared user accounts to determine that shared user accounts within the badge access control and video surveillance applications were prohibited unless documented approval was obtained and documented via a standard exception form.	No exceptions noted.
		Inspected the standard exception form for a sample of shared user accounts within the badge access control and video surveillance applications to determine that each shared user account sampled had an approved standard exception form.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.3.5	Administrative access privileges within the badge access control and video surveillance applications are restricted to user accounts accessible by authorized security personnel.	Inspected the administrator user account listings for the in-scope badge access control and video surveillance applications with the assistance of the senior information security auditor to determine that administrative access privileges were restricted to user accounts accessible by authorized security personnel.	No exceptions noted.
CC6.3.6	The ability to create, modify, or remove badge access users and privileges is restricted to administrator user accounts accessible by authorized security personnel.	Inspected the badge access control system administrator user account listing with the assistance of the senior information security auditor to determine that the ability to create, modify, or remove badge access privileges was restricted to administrator user accounts accessible by authorized security personnel.	No exceptions noted.
CC6.3.7	Logical user access reviews are performed on an annual basis to help ensure that access to the badge access control and video surveillance applications is restricted.	Inspected the most recently completed logical user access review for the in-scope badge access control and video surveillance applications to determine that an access review was performed during the period.	No exceptions noted.
CC6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.			
CC6.4.1	Physical security policies and procedures are in place to guide personnel in the following areas: · Data center access for employees, contractors, and visitors · Security monitoring · Security assessments and access activity reviews	Inspected the physical security policies and procedures to determine that documented physical security policies and procedures were in place to guide personnel in the following areas: · Data center access for employees, contractors, and visitors · Security monitoring · Security assessments and access activity reviews	No exceptions noted.
CC6.4.2	Security access controls (i.e., physical barriers and doors, card-controlled entry points, biometric scanning, video surveillance and/or manned reception desks) are utilized to protect areas that contain information and information processing facilities.	Observed the access controls for a sample of in-scope data center facilities to determine that security access controls (i.e., physical barriers and doors, card-controlled entry points, biometric scanning, video surveillance and/or manned reception desks) were utilized to protect areas that contain information and information processing facilities.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.4.3	Access to the Lumen common areas and data centers is restricted via a badge access control system.	Observed the access controls for a sample of in-scope data center facilities to determine that access to the Lumen common areas and data centers was restricted via a badge access control system.	No exceptions noted.
CC6.4.4	Control mechanisms are in place to limit physical access to restricted data center areas such as the raised floor, equipment rooms, transport areas, and critical power and mechanical infrastructure.	Observed the access controls for a sample of in-scope data center facilities to determine that control mechanisms were in place to limit physical access to restricted data center areas such as the raised floor, equipment rooms, transport areas, and critical power and mechanical infrastructure.	No exceptions noted.
CC6.4.5	The badge access control system is configured to log successful and unsuccessful activity traceable to individual cardholders and activity logs are retained for a minimum of 90 days.	Inspected the badge access control system activity logs generated during the period for a sample of in-scope data center facilities to determine that the badge access control system was configured to log successful and unsuccessful activity traceable to individual cardholders and that activity logs were retained for a minimum of 90 days.	No exceptions noted.
CC6.4.6	The ability to create, modify, or remove badge access users and privileges is restricted to administrator user accounts accessible by authorized security personnel.	Inspected the badge access control system administrator user account listing with the assistance of the manager of physical security and operations to determine that the ability to create, modify, or remove badge access privileges was restricted to administrator user accounts accessible by authorized security personnel.	No exceptions noted.
CC6.4.7	Data center access for Lumen personnel is revoked as a component of the employee termination process.	Inspected the badge access control system user listing for a sample of in-scope data center facilities and employees terminated during the period to determine that data center access for Lumen personnel was revoked as a component of the employee termination process.	No exceptions noted.
CC6.4.8	Physical user access reviews are performed on an annual basis to help ensure that access to the data center facilities is restricted to authorized personnel.	Inspected the most recent annual physical access review documentation for a sample of in-scope data center facilities to determine that an access review was performed during the period to help ensure that access to the data center facilities was restricted to authorized personnel.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.4.9	Visitor (and contractor) access must be pre-approved by authorized Lumen and/or customer personnel prior to granting facility access.	Inspected the visitation ticket for a sample of visitors granted access to each of the in-scope data center facilities during the period to determine that access was pre-approved by authorized Lumen and/or customer personnel prior to granting facility access for each visitor sampled.	No exceptions noted.
CC6.4.10	Persons entering the data centers must present valid government-issued photo ID or display and use a valid Lumen photo access badge prior to entering the facility.	Observed the visitor entrance procedures for a sample of in-scope data center facilities to determine that persons entering the data centers were required to present valid government-issued photo ID or displayed and used a valid Lumen photo access badge prior to entering the facility.	No exceptions noted.
CC6.4.11	Visitors are required to be escorted by an authorized Lumen employee or authorized customer representative at all times while in the data centers.	Observed the visitor entrance procedures for a sample of in-scope data center facilities to determine that visitors were required to be escorted by an authorized Lumen employee or authorized customer representative while in the data centers.	No exceptions noted.
CC6.4.12	Visitor logs are maintained for at least 90 days to document visitor activity at the data centers.	Inspected the historical visitation ticket log for a sample of in-scope data center facilities during the period to determine that visitor logs were maintained for a minimum of 90 days to document visitor activity.	No exceptions noted.
CC6.4.13	Surveillance cameras are utilized to monitor access to the office buildings and data centers and are located at entrances and exits to the data center raised floor / production areas.	Inquired of the security compliance auditor regarding facility monitoring to determine that surveillance cameras were utilized to monitor access to the office buildings and data centers and were located at entrances and exits to the data center raised floor / production areas.	No exceptions noted.
		Observed the presence of surveillance cameras for a sample of in-scope data center facilities to determine that surveillance cameras were utilized to monitor access to the office buildings and data centers and were located at entrances and exits to the data center raised floor / production areas.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the surveillance camera placement maps for a sample of in-scope data center facilities to determine that surveillance cameras were in place to monitor access to the office buildings and data centers and were located at entrances and exits to the data center raised floor / production areas.	Refer to the test results for control activity CC4.1.1.
CC6.4.14	CCTV surveillance video and/or ACS activity logs are retained for a minimum of 90 calendar days.	Inspected the historical recordings from the surveillance cameras and/or the badge access control system activity logs for a sample of in-scope data center facilities during the period to determine that CCTV surveillance video and/or ACS activity logs were retained for a minimum of 90 calendar days.	No exceptions noted.
CC6.4.15	Data center security personnel and the PSOC monitor access to the data centers 24 hours a day, seven days a week, using reports from the physical security access mechanisms, alarms, and CCTV video surveillance systems.	Inquired of the security compliance auditor regarding facility monitoring to determine that data center security personnel and the PSOC monitored access to the data centers 24 hours a day, seven days a week, using reports from the physical security access mechanisms, alarms, and CCTV video surveillance systems.	No exceptions noted.
		Inspected the PSOC staffing schedules during the period to determine that PSOC personnel were staffed 24 hours per day, seven days per week.	No exceptions noted.
CC6.5 The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.			
CC6.5.1	Documented data retention and destruction policies and procedures are in place to define retention periods and destruction procedures for confidential data.	Inspected the data retention and destruction policies and procedures to determine that retention periods and destruction procedures were defined for confidential data.	No exceptions noted.
CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC6.6.1	Policies are in place that prohibit the transmission of sensitive information over the Internet or other public communications paths unless it is encrypted.	Inspected the data encryption policies to determine that policies were in place that prohibited the transmission of sensitive information over the Internet or other public communications paths unless it was encrypted.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.6.2	Web servers utilize TLS encryption for web communication sessions.	Inspected the TLS encryption settings to determine that web servers utilized TLS encryption for web communication sessions.	The test of the control activity disclosed that Control Center allowed deprecated versions of the TLS protocol (i.e., TLS 1.0 and TLS 1.1) for web communication sessions.
CC6.7 The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.			
CC6.7.1	Policies are in place that prohibit the transmission of sensitive information over the Internet or other public communications paths unless it is encrypted.	Inspected the data encryption policies to determine that policies were in place that prohibited the transmission of sensitive information over the Internet or other public communications paths unless it was encrypted.	No exceptions noted.
CC6.7.2	Web servers utilize TLS encryption for web communication sessions.	Inspected the TLS encryption settings to determine that web servers utilized TLS encryption for web communication sessions.	Refer to the test results for control activity CC6.6.2.
CC6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
CC6.8.1	Policies and procedures are in place that prohibit the installation of non-approved software on employee workstations.	Inspected the information security policy to determine that policies and procedures were in place that prohibited the installation of non-approved software on employee workstations.	No exceptions noted.
CC6.8.2	A central antivirus server is configured with antivirus software to protect registered production servers and workstations supporting the badge access control and video surveillance applications.	Inspected the enterprise antivirus software configurations to determine that enterprise antivirus software was installed on production servers and workstations supporting the badge access control applications.	No exceptions noted.
System Operations			
CC7.1 To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.			
CC7.1.1	Documented policies and procedures are in place to guide personnel in the design, development, implementation, operation, maintenance, and monitoring of in-scope systems.	Inspected the corporate security policies and procedures to determine that documented policies and procedures were in place to guide personnel in the design, development, implementation, operation, maintenance, and monitoring of in-scope systems.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.1.2	A BMS is configured to monitor data center equipment including, but not limited to, the following: · Fire alarm status and suppression systems · Temperature and humidity levels · Power levels and availability	Inspected the BMS configurations to determine that a BMS was utilized to monitor data center equipment including, but not limited to, the following: · Fire alarm status and suppression systems · Temperature and humidity levels · Power levels and availability	No exceptions noted.
CC7.1.3	The BMS is integrated with the ticketing system and configured to generate a ticket and alert local field operations personnel when predefined thresholds are exceeded on monitored devices.	Inspected the BMS configurations and an example alert generated during the period to determine that a BMS was integrated with the ticketing system and configured to generate a ticket and alert local field operations personnel when predefined thresholds were exceeded on monitored devices.	No exceptions noted.
CC7.1.4	Surveillance cameras are utilized to monitor access to the office buildings and data centers and are located at entrances and exits to the data center raised floor / production areas.	Inquired of the security compliance auditor regarding facility monitoring to determine that surveillance cameras were utilized to monitor access to the office buildings and data centers and were located at entrances and exits to the data center raised floor / production areas.	No exceptions noted.
		Observed the presence of surveillance cameras for a sample of in-scope data center facilities to determine that surveillance cameras were utilized to monitor access to the office buildings and data centers and were located at entrances and exits to the data center raised floor / production areas.	No exceptions noted.
		Inspected the surveillance camera placement maps for a sample of in-scope data center facilities to determine that surveillance cameras were in place to monitor access to the office buildings and data centers and were located at entrances and exits to the data center raised floor / production areas.	Refer to the test results for control activity CC4.1.1.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.1.5	Data center security personnel and the PSOC monitor access to the data centers 24 hours a day, seven days a week, using reports from the physical security access mechanisms, alarms, and CCTV video surveillance systems.	Inquired of the security compliance auditor regarding facility monitoring to determine that data center security personnel and the PSOC monitored access to the data centers 24 hours a day, seven days a week, using reports from the physical security access mechanisms, alarms, and CCTV video surveillance systems.	No exceptions noted.
		Inspected the PSOC staffing schedules during the period to determine that PSOC personnel were staffed 24 hours per day, seven days per week.	No exceptions noted.
CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.			
CC7.2.1	Documented policies and procedures are in place to guide personnel in the design, development, implementation, operation, maintenance, and monitoring of in-scope systems.	Inspected the corporate security policies and procedures to determine that documented policies and procedures were in place to guide personnel in the design, development, implementation, operation, maintenance, and monitoring of in-scope systems.	No exceptions noted.
CC7.2.2	Surveillance cameras are utilized to monitor access to the office buildings and data centers and are located at entrances and exits to the data center raised floor / production areas.	Inquired of the security compliance auditor regarding facility monitoring to determine that surveillance cameras were utilized to monitor access to the office buildings and data centers and were located at entrances and exits to the data center raised floor / production areas.	No exceptions noted.
		Observed the presence of surveillance cameras for a sample of in-scope data center facilities to determine that surveillance cameras were utilized to monitor access to the office buildings and data centers and were located at entrances and exits to the data center raised floor / production areas.	No exceptions noted.
		Inspected the surveillance camera placement maps for a sample of in-scope data center facilities to determine that surveillance cameras were in place to monitor access to the office buildings and data centers and were located at entrances and exits to the data center raised floor / production areas.	Refer to the test results for control activity CC4.1.1.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.2.3	A BMS is configured to monitor data center equipment including, but not limited to, the following: · Fire alarm status and suppression systems · Temperature and humidity levels · Power levels and availability	Inspected the BMS configurations to determine that a BMS was utilized to monitor data center equipment including, but not limited to, the following: · Fire alarm status and suppression systems · Temperature and humidity levels · Power levels and availability	No exceptions noted.
CC7.2.4	Data center security personnel and the PSOC monitor access to the data centers 24 hours a day, seven days a week, using reports from the physical security access mechanisms, alarms, and CCTV video surveillance systems.	Inquired of the security compliance auditor regarding facility monitoring to determine that data center security personnel and the PSOC monitored access to the data centers 24 hours a day, seven days a week, using reports from the physical security access mechanisms, alarms, and CCTV video surveillance systems.	No exceptions noted.
		Inspected the PSOC staffing schedules during the period to determine that PSOC personnel were staffed 24 hours per day, seven days per week.	No exceptions noted.
CC7.2.5	The BMS is integrated with the ticketing system and configured to generate a ticket and alert local field operations personnel when predefined thresholds are exceeded on monitored devices.	Inspected the BMS configurations and an example alert generated during the period to determine that a BMS was integrated with the ticketing system and configured to generate a ticket and alert local field operations personnel when predefined thresholds were exceeded on monitored devices.	No exceptions noted.
CC7.2.6	Security access controls (i.e., physical barriers and doors, card-controlled entry points, biometric scanning, video surveillance and/or manned reception desks) are utilized to protect areas that contain information and information processing facilities.	Observed the access controls for a sample of in-scope data center facilities to determine that security access controls (i.e., physical barriers and doors, card-controlled entry points, biometric scanning, video surveillance and/or manned reception desks) were utilized to protect areas that contain information and information processing facilities.	No exceptions noted.
CC7.2.7	Access to the Lumen common areas and data centers is restricted via a badge access control system.	Observed the access controls for a sample of in-scope data center facilities to determine that access to the Lumen common areas and data centers was restricted via a badge access control system.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.2.8	Control mechanisms are in place to limit physical access to restricted data center areas such as the raised floor, equipment rooms, transport areas, and critical power and mechanical infrastructure.	Observed the access controls for a sample of in-scope data center facilities to determine that control mechanisms were in place to limit physical access to restricted data center areas such as the raised floor, equipment rooms, transport areas, and critical power and mechanical infrastructure.	No exceptions noted.
CC7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.			
CC7.3.1	Documented policies and procedures are in place to guide personnel in the design, development, implementation, operation, maintenance, and monitoring of in-scope systems.	Inspected the corporate security policies and procedures to determine that documented policies and procedures were in place to guide personnel in the design, development, implementation, operation, maintenance, and monitoring of in-scope systems.	No exceptions noted.
CC7.3.2	Service guides are provided to external users to guide users in reporting security and availability failures, incidents, concerns, and other complaints.	Inspected the data center user guide to determine that service guides were provided to external users to guide users in reporting security and availability failures, incidents, concerns, and other complaints.	No exceptions noted.
CC7.3.3	Management meetings are held on a monthly basis to discuss security incidents and corrective measures to help ensure that incidents are resolved.	Inspected the management meeting minutes for a sample of months during the period to determine that management meetings were held to discuss security incidents and corrective measures to help ensure incidents were resolved for each month sampled.	No exceptions noted.
CC7.3.4	Data center security personnel and the PSOC monitor access to the data centers 24 hours a day, seven days a week, using reports from the physical security access mechanisms, alarms, and CCTV video surveillance systems.	Inquired of the security compliance auditor regarding facility monitoring to determine that data center security personnel and the PSOC monitored access to the data centers 24 hours a day, seven days a week, using reports from the physical security access mechanisms, alarms, and CCTV video surveillance systems.	No exceptions noted.
		Inspected the PSOC staffing schedules during the period to determine that PSOC personnel were staffed 24 hours per day, seven days per week.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
CC7.4.1	Documented escalation procedures for security and availability incidents are provided to internal users to guide users in identifying and reporting failures, incidents, concerns, and other complaints.	Inspected the incident response and escalation procedures to determine that documented escalation procedures for reporting security and availability incidents were provided to internal users to guide users in identifying and reporting failures, incidents, concerns, and other complaints.	No exceptions noted.
CC7.4.2	Employee roles and responsibilities are documented within the incident response policies and procedures.	Inspected the incident response policies and procedures to determine that employee roles and responsibilities were documented within the incident response policies and procedures.	No exceptions noted.
CC7.4.3	Management meetings are held on a monthly basis to discuss security incidents and corrective measures to help ensure that incidents are resolved.	Inspected the management meeting minutes for a sample of months during the period to determine that management meetings were held to discuss security incidents and corrective measures to help ensure incidents were resolved for each month sampled.	No exceptions noted.
CC7.4.4	An automated ticketing system is utilized to document security and availability incidents, responses, and resolution activities.	Inspected the automated incident ticket generation configurations to determine that an automated ticketing system was utilized to document security and availability incidents, responses, and resolution activities.	No exceptions noted.
CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.			
CC7.5.1	Documented incident response procedures are in place to guide the incident response process and include the following: · Remediation of the incident · Restoration of operations · Communication protocols and timing to affected parties · Lessons learned	Inspected the incident response policies and procedures to determine that documented procedures were in place to guide the incident response process and included the following: · Remediation of the incident · Restoration of operations · Communication protocols and timing to affected parties · Lessons learned	No exceptions noted.
CC7.5.2	Management meetings are held on a monthly basis to discuss security incidents and corrective measures to help ensure that incidents are resolved.	Inspected the management meeting minutes for a sample of months during the period to determine that management meetings were held to discuss security incidents and corrective measures to help ensure incidents were resolved for each month sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.5.3	An automated ticketing system is utilized to document security and availability incidents, responses, and resolution activities.	Inspected the automated incident ticket generation configurations to determine that an automated ticketing system was utilized to document security and availability incidents, responses, and resolution activities.	No exceptions noted.
Change Management			
CC8.1 The entity authorizes, designs, develops, or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
CC8.1.1	Change management policies and procedures are in place to guide personnel in patch management processes.	Inspected the change management policies and procedures to determine that change management policies and procedures were in place to guide personnel in patch management processes.	No exceptions noted.
CC8.1.2	Patches are applied to in-scope systems on a monthly basis.	Inspected the patching ticket for a sample of months during the period to determine that patches were applied to the in-scope systems for each month sampled.	No exceptions noted.
CC8.1.3	Access privileges to configure and implement patches to in-scope systems are restricted to user accounts accessible by authorized personnel.	Inspected the administrator user account listings for the in-scope badge access control and video surveillance applications with the assistance of the senior information security auditor to determine that access privileges to configure and implement patches to in-scope systems were restricted to user accounts accessible by authorized personnel.	No exceptions noted.
CC8.1.4	A change ticketing system is in place to centrally document, manage, and monitor changes from change request through implementation.	Inspected patching ticket for a sample of months during the period to determine that a change ticketing system was in place to centrally document, manage, and monitor changes from change request through implementation.	No exceptions noted.
CC8.1.5	Changes made to in-scope systems are documented and approved prior to implementation.	Inspected patching documentation for a sample of monthly patches during the period to determine that changes made to in-scope systems were documented and approved prior to implementation for each month sampled.	No exceptions noted.
CC8.1.6	A change management meeting is held on a weekly basis to discuss and communicate the ongoing and upcoming projects that affect the system.	Inspected the recurring calendar invite and an example agenda for the technical advisory group meeting to determine that a change management meeting was held on a weekly basis to discuss and communicate the ongoing and upcoming projects that affect the system.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
Risk Mitigation			
CC9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
CC9.1.1	Documented policies and procedures are in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk mitigation strategies as a part of the risk assessment process.	Inspected the risk management policies and procedures to determine that policies and procedures were in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk mitigation strategies as a part of the risk assessment process.	No exceptions noted.
CC9.1.2	A risk assessment is performed on an annual basis that considers risks arising from potential business disruptions. Identified risks are rated using a risk evaluation process and are formally documented, with mitigation strategies, for management review.	Inspected the most recent risk assessment to determine that a risk assessment was performed during the period that considered risks arising from potential business disruptions and identified risks were rated using a risk evaluation process and were formally documented, with mitigation strategies, for management review.	No exceptions noted.
CC9.1.3	Risk mitigation activities consider the use of insurance to offset the financial impact of loss events that would otherwise impair the ability of Lumen to meet its objectives.	Inspected the third-party cyber insurance policy to determine that risk management activities considered the use of insurance to offset the financial impact of loss events that would impair the ability of Lumen to meet its objectives.	No exceptions noted.
CC9.2 The entity assesses and manages risks associated with vendors and business partners.			
CC9.2.1	Policies and procedures are in place to guide personnel in the identification, monitoring, and audit of third-party providers.	Inspected the vendor risk management policies and procedures to determine that policies and procedures were in place to guide personnel in the identification, monitoring, and audit of third-party vendors.	No exceptions noted.
CC9.2.2	Confidentiality agreements are required to be in place with third parties prior to sharing information designated as confidential.	Inspected the confidentiality agreement for the subservice organizations to determine that confidentiality agreements were in place with third parties prior to sharing information designated as confidential.	No exceptions noted.
CC9.2.3	Third parties are screened, and associated risks are evaluated by Lumen prior to onboarding.	Observed the company website and prospective supplier registration form with the assistance of the senior information security auditor to determine that third parties were screened, and associated risks were evaluated by Lumen prior to onboarding.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the vendor management procedures to determine that third parties were screened, and associated risks were evaluated by Lumen prior to onboarding.	No exceptions noted.
CC9.2.4	The compliance team performs vendor audit report reviews and/or vendor security assessments on an annual basis to ensure that vendors are in compliance with Lumen's requirements.	Inspected the vendor audit report review and/or the vendor security assessment for a sample of vendors during the period to determine that the compliance team performed vendor audit report reviews and/or vendor security assessments during the period to ensure that vendors were in compliance with Lumen's requirements.	No exceptions noted.

ADDITIONAL CRITERIA FOR AVAILABILITY

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.1 The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.			
A1.1.1	A BMS is configured to monitor data center equipment including, but not limited to, the following: · Fire alarm status and suppression systems · Temperature and humidity levels · Power levels and availability	Inspected the BMS configurations to determine that a BMS was utilized to monitor data center equipment including, but not limited to, the following: · Fire alarm status and suppression systems · Temperature and humidity levels · Power levels and availability	No exceptions noted.
A1.1.2	The BMS is integrated with the ticketing system and configured to generate a ticket and alert local field operations personnel when predefined thresholds are exceeded on monitored devices.	Inspected the BMS configurations and an example alert generated during the period to determine that a BMS was integrated with the ticketing system and configured to generate a ticket and alert local field operations personnel when predefined thresholds were exceeded on monitored devices.	No exceptions noted.
A1.1.3	Management meetings are held on a monthly basis to review availability trends and availability forecasts as compared to system commitments.	Inspected the management meeting minutes for a sample of months during the period to determine that management meetings were held each month sampled to review availability trends and forecasts as compared to system commitments.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.2 The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.			
A1.2.1	Environmental security policies and procedures are in place to guide personnel in the following areas: · Equipment specifications and operating instructions · Equipment inspections · Preventative maintenance schedules	Inspected the environmental security policies and procedures to determine that documented environmental security policies and procedures were in place to guide personnel in the following areas: · Equipment specifications and operating instructions · Equipment inspections · Preventative maintenance schedules	No exceptions noted.
A1.2.2	Fire detection and suppression equipment is in place at each data center.	Observed the fire detection and suppression equipment for a sample of in-scope data center facilities to determine that the data centers were equipped with fire detection and suppression devices.	No exceptions noted.
A1.2.3	The data centers are equipped with multiple CRAC/HVAC units configured to regulate temperature and humidity levels.	Observed the CRAC/HVAC units for a sample of the in-scope data center facilities to determine that multiple CRAC/HVAC units were in place to regulate temperature and humidity levels.	No exceptions noted.
A1.2.4	Power management equipment is in place at each data center.	Observed the UPS systems and generators for a sample of in-scope data center facilities to determine that power management equipment was in place at each data center.	No exceptions noted.
A1.2.5	Servers are maintained in racks to facilitate cooling and protect equipment from localized flooding.	Observed server placement for a sample of in-scope data center facilities to determine that servers were maintained in racks to facilitate cooling and protect equipment from localized flooding.	No exceptions noted.
A1.2.6	Water detection systems are in place to detect leakage from the CRAC/HVAC units.	Observed the water detection systems located for a sample of in-scope data center facilities to determine that water detection systems were in place to detect leakage from the CRAC/HVAC units.	No exceptions noted.
A1.2.7	A BMS is configured to monitor data center equipment including, but not limited to, the following: · Fire alarm status and suppression systems · Temperature and humidity levels · Power levels and availability	Inspected the BMS configurations to determine that a BMS was utilized to monitor data center equipment including, but not limited to, the following: · Fire alarm status and suppression systems · Temperature and humidity levels · Power levels and availability	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.2.8	The BMS is integrated with the ticketing system and configured to generate a ticket and alert local field operations personnel when predefined thresholds are exceeded on monitored devices.	Inspected the BMS configurations and an example alert generated during the period to determine that a BMS was integrated with the ticketing system and configured to generate a ticket and alert local field operations personnel when predefined thresholds were exceeded on monitored devices.	No exceptions noted.
A1.2.9	Third-party specialists inspect power management systems according to a predefined maintenance schedule.	Inspected the most recent UPS system inspection reports for a sample of in-scope data center facilities to determine that third-party specialists inspected UPS systems during the period for each data center sampled.	The test of the control activity disclosed that third-party specialists did not inspect the UPS systems during the period for the following six (6) of 24 data center facilities sampled: · Baltimore · Little Rock · Pittsburgh · Reno · San Antonio · West Sacramento
		Inspected the most recent generator inspection reports for a sample of in-scope data center facilities to determine that that third-party specialists inspected generators on a biennial basis for each data center sampled.	Inspected the most recent generator inspection report for a sample of in-scope data centers and determined that generator inspections were not scheduled to be performed during the period for 13 of 24 sampled data centers; therefore, no testing of operating effectiveness was performed. Of the 16 data center facilities scheduled for a biennial inspection, the test of the control activity disclosed that third-party specialists did not inspect the generators during the period for the following one (1) data center facility sampled: Boise No exceptions noted for the remaining 15 of 24 data center facilities sampled and scheduled to undergo biennial maintenance during the period.
A1.2.10	Third-party specialists inspect fire detection and suppression systems on an annual basis.	Inspected the most recent fire detection and suppression system inspection reports for a sample of in-scope data center facilities to determine that third-party specialists inspected fire detection and suppression systems during the period for each data center sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.2.11	Field engineers and/or third-party specialists inspect the CRAC/HVAC units on at least an annual basis.	Inspected the most recent CRAC/HVAC unit inspection reports for a sample of in-scope data center facilities to determine that field engineers and/or third-party specialists inspected the CRAC/HVAC units during the period for each data center facility sampled.	The test of the control activity disclosed that field engineers and/or third-party specialists did not inspect the CRAC/HVAC units during the period for the following one (1) of 24 data center facilities sampled: San Antonio
A1.2.12	Automated backup systems are in place to perform scheduled backups of production servers supporting the badge access control systems at predefined times.	Inspected the automated backup system configurations to determine that automated backup systems were in place to perform scheduled backups of production servers supporting the badge access control systems at predefined times.	No exceptions noted.
A1.2.13	The automated backup systems are configured to send alert notifications to IT personnel regarding backup job failures.	Inspected the automated backup system configurations and an example alert generated during the period to determine that the automated backup systems were configured to send alert notifications to IT personnel regarding backup job failures.	No exceptions noted.
A1.2.14	Disaster recovery plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.	Inspected the business continuity and disaster recovery plan for a sample of in-scope data center facilities to determine that disaster recovery plans were in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.	No exceptions noted.
	Third-party building management companies at the New York City (8th Ave) and Omaha data center facilities are responsible for performing regular preventative maintenance inspections according to a predefined schedule for environmental control systems owned and managed by the building management companies.		
A1.3 The entity tests recovery plan procedures supporting system recovery to meet its objectives.			
A1.3.1	Disaster recovery and business continuity plans are evaluated and tested on at least an annual basis.	Inspected the results of the most recent annual disaster recovery test for a sample of in-scope data center facilities to determine that disaster recovery and business continuity plans were evaluated and tested during the period.	No exceptions noted.

SECTION 5

OTHER INFORMATION PROVIDED BY LUMEN

MANAGEMENT'S RESPONSE TO TESTING EXCEPTIONS

Security

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC4.1.1 CC6.4.13 CC7.1.4 CC7.2.2	Surveillance cameras are utilized to monitor access to the office buildings and data centers and are located at entrances and exits to the data center raised floor / production areas.	Inspected the surveillance camera placement maps for a sample of in-scope data center facilities to determine that surveillance cameras were in place to monitor access to the office buildings and data centers and were located at entrances and exits to the data center raised floor / production areas.	The test of the control activity disclosed that a surveillance camera placement map was not in place for the following one (1) of 24 data center facilities sampled: Newark
Management's Response:	A new camera system was installed at this location resulting in changes to the camera placement map. An updated AutoCAD map is being completed and will be uploaded to the camera map library by 8-1-2022.		
CC6.6.2 CC6.7.2	Web servers utilize TLS encryption for web communication sessions.	Inspected the TLS encryption settings to determine that web servers utilized TLS encryption for web communication sessions.	The test of the control activity disclosed that Control Center allowed deprecated versions of the TLS protocol (i.e., TLS 1.0 and TLS 1.1) for web communication sessions.
Management's Response:	TLS 1.0 and TLS 1.1 protocols are no longer supported. The environment is currently locked down to allow TLS 1.2 only. This change was made on our load balancer which is terminating the TLS/SSL connections.		

Availability

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.2.9	Third-party specialists inspect power management systems according to a predefined maintenance schedule.	Inspected the most recent UPS system inspection reports for a sample of in-scope data center facilities to determine that third-party specialists inspected UPS systems during the period for each data center sampled.	The test of the control activity disclosed that third-party specialists did not inspect the UPS systems during the period for the following six (6) of 24 data center facilities sampled: · Baltimore · Little Rock · Pittsburgh · Reno · San Antonio · West Sacramento

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the most recent generator inspection reports for a sample of in-scope data center facilities to determine that that third-party specialists inspected generators on a biennial basis for each data center sampled.	Inspected the most recent generator inspection report for a sample of in-scope data centers and determined that generator inspections were not scheduled to be performed during the period for 13 of 24 sampled data centers; therefore, no testing of operating effectiveness was performed. Of the 16 data center facilities scheduled for a biennial inspection, the test of the control activity disclosed that third-party specialists did not inspect the generators during the period for the following one (1) data center facility sampled: Boise No exceptions noted for the remaining 15 of 24 data center facilities sampled and scheduled to undergo biennial maintenance during the period.
Management's Response:	UPS: Baltimore, Pittsburgh, San Antonio, and West Sacramento were all delayed due to vendor resource issues that began in early spring. Pittsburgh and San Antonio were completed in early June 2022. West Sacramento will be completed July 2022 and Baltimore will be completed in August 2022. We are working closely with the vendor to ensure timely completion of all open annual inspections. More frequent discussions regarding scheduling issues are being implemented to ensure the annual inspections are completed between January and April, and semi-annual inspections are completed 6 months after. Operations management is working directly with the vendors to ensure timely scheduled inspections. Little Rock and Reno are newly installed units. The units were not scheduled for inspection until late April, missing the testing window. Future new installs will be scheduled within the appropriate testing window to ensure inspections are completed. Generator: Boise was a new site introduction in 2022 due to Edge being pulled into scope. Appropriate scheduling will occur the same as stated above in UPS.		
A1.2.11	Field engineers and/or third-party specialists inspect the CRAC/HVAC units on at least an annual basis.	Inspected the most recent CRAC/HVAC unit inspection reports for a sample of in-scope data center facilities to determine that field engineers and/or third-party specialists inspected the CRAC/HVAC units during the period for each data center facility sampled.	The test of the control activity disclosed that field engineers and/or third-party specialists did not inspect the CRAC/HVAC units during the period for the following one (1) of 24 data center facilities sampled: San Antonio
Management's Response:	The local vendor was not able to gain access to the facility in May, and the inspection was completed in early June. All HVAC inspections going forward will be scheduled prior to May 1.		