January 8, 2024

SCO Cloud
Attn: Robert Ungaretti
PO BOX 689
Armonk, NY 10504

Robert:

Switch, Ltd. ("Switch") engaged Schellman & Company, LLC. (Schellman) to issue a report regarding our service organization based on Statements on Standards for Attestation Engagements (SSAE) No. 18, Service Organization Control (SOC)-1, Type 2 "Report on management's description of a service organization's system and the suitability of the design and operating effectiveness of controls" for the period October 1, 2022 through September 30, 2023, and SOC-2 "Report on Controls Relevant to Security and Availability".

Schellman issued an annual SSAE-18 SOC-1 Type 2 and SOC-2 to Switch in November 2023, and the Auditor's Report was made available and provided to your firm. Switch regularly reviews and tests our internal controls and procedures. This information and the test results are shared with and reviewed by Schellman to assist them with their SSAE-18 SOC-1 Type 2 and SOC-2 reviews.

You should also be aware that Switch, as a normal part of its operations, continually updates its services and technology as appropriate. In addition, the controls for Switch's services were designed with certain responsibilities required of the service users. Switch's controls must be evaluated in conjunction with an assessment of user compliance with such responsibilities.

To the best of our knowledge, there have not been any significant changes in the internal controls described in the SSAE-18, SOC-1 Type 2 and SOC-2 since it was issued for the period ending September 30, 2023, or any material weaknesses in such internal controls and procedures that require any corrective action. Please contact me if you have any questions.

Sincerely,
Switch

Joseph A. Smith
Investigations Manager

SWITCH, LTD.

INDEPENDENT PRACTITIONER'S REPORT ON THE INFORMATION SECURITY PROGRAM FOR THE SWITCH COLOCATION SERVICES RELATED TO HIPAA AND HITECH

SEPTEMBER 30, 2023

Attestation and Compliance Services

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

If the 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 I

INDEPENDENT PRACTITIONER'S REPORT

INDEPENDENT PRACTITIONER'S REPORT

To Switch, Ltd.:

Scope

We have examined Switch, Ltd.'s ("Switch") management's assertion that the description of its information security program supporting the Switch Colocation Services system that was provided to customer organizations (or "user entities") as of September 30, 2023, and included in Section 3 (the "description"), is fairly presented and that the information security program conforms, as of September 30, 2023, to the applicable implementation specifications within the Health Insurance Portability and Accountability Act ("HIPAA") Security Standards for the Protection of Electronic Protected Health Information ("HIPAA Security Rule") and the Notification in the Case of Breach of Unsecured Protected Health Information enacted as part of the American Recovery and Reinvestment Act of 2009 ("HITECH Breach Notification Requirements"), as described in Part 164 of CFR 45, in accordance with the criteria set forth in Section 2 ("management's assertion").

In Section 5, Switch has provided additional information that is not a part of Switch's description. Such information has not been subjected to the procedures applied in our examination, and accordingly, we express no opinion on it.

Switch's Responsibilities

Switch has provided the attached assertion, in Section 2, about the fairness of the presentation of the description based on the description criteria. Switch is responsible for preparing the description and the assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services and related controls covered by the description; determining the applicability of the implementation specifications; and implementing the controls described therein for conformance of its information security program to meet the HIPAA Security Rule and HITECH Breach Notification criteria.

Independent Practitioner's Responsibilities

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

Inherent Limitations

Our organization is a licensed and independent CPA firm; however, our examination does not constitute a legal determination of compliance with the relevant regulations or a substitute for audit procedures that may be applied separately by regulatory entities. The specific procedures we performed, the nature, timing, and results of our tests are presented in Section 4 of our report titled "Results."

Because of their nature, controls may not prevent, or detect and correct, all errors or omissions relevant to the information security program. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the effectiveness of the information security program, is subject to the risk that controls may become inadequate or fail.

Opinion

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

a. the description fairly presents the information security program supporting the Switch Colocation Services system that was provided to user entities, as of September 30, 2023; and

b. the information security program conformed to the applicable implementation specifications within the HIPAA Security Rule and the HITECH Breach Notification Requirements, as described in Part 164 of CFR 45, as of September 30, 2023.

Restricted Use

This report, including the Results, is intended solely for the information and use of Switch and user entities of the Switch Colocation Services system that was provided to user entities as of September 30, 2023, who have sufficient knowledge and understanding of the following:

- **the nature of the service provided by Switch;**
- **the nature of the data provided to Switch and the definition of protected health information;**
- **how Switch's system interacts with user entities;**
- **internal control and its limitations;**
- **the applicable HIPAA Security Rule and HITECH Breach Notification Requirements; and**
- **the risks that may threaten the achievement of the applicable HIPAA Security Rule and HITECH Breach Notification 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
November 8, 2023

SECTION 2

MANAGEMENT'S ASSERTION

switch

MANAGEMENT'S ASSERTION

We have prepared the description of Switch, Ltd.'s ("Switch") information security program supporting the Switch Colocation Services system that was provided to customer organizations (or "user entities") as of September 30, 2023. We confirm, to the best of our knowledge, that:

a. the description fairly presents the Switch Colocation Services system made available to user entities of the system as of September 30, 2023. The criteria we used in making this assertion were that the description:

   i. presents how the information security program was designed and implemented to govern the security policies and practices supporting the Switch Colocation Services system;

   ii. describes the relevant safeguards, standards, and rules deemed applicable by management;

   iii. describes the specified controls within the information security program designed to achieve the information security program's objectives (the "Controls"); and

   iv. does not omit or distort information relevant to the information security program, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system, and may not, therefore, include every aspect of the Switch Colocation Services system that each individual user entity of the system and its auditor may consider important in its own particular environment; and

b. the information security program supporting the Switch Colocation Services system conforms, as of September 30, 2023, to the applicable implementation specifications within the Health Insurance Portability and Accountability Act ("HIPAA") Security Standards for the Protection of Electronic Protected Health Information ("HIPAA Security Rule") and the Notification in the Case of Breach of Unsecured Protected Health Information enacted as part of the American Recovery and Reinvestment Act of 2009 ("HITECH Breach Notification Requirements"), as described in Part 164 of CFR 45. The criteria we used in making this assertion were that:

   i. management determined the applicable Controls included in the information security program;

   ii. the Controls, as described, met implementation specifications for the applicable safeguards, standards, and rules, as defined in HIPAA Security Rule and HITECH Breach Notification Requirements; and

   iii. the Controls, as described, were implemented as of September 30, 2023.

Section 3 of this report includes Switch description of its Switch Colocation Services system that is covered by this assertion.

SECTION 3

DESCRIPTION OF THE INFORMATION SECURITY PROGRAM

OVERVIEW OF OPERATIONS

Company Background

Switch is a technology infrastructure ecosystem corporation whose core business is the design, construction, and operation of data centers. Founded in 2000 and headquartered in Las Vegas, Nevada, Switch is built on the intelligent and sustainable growth of the Internet. The Founder and CEO, Rob Roy, has developed more than 700 issued and pending patent claims covering data center designs that manifested into Switch data centers and technology solution ecosystems. Since the opening of their first colocation facility, Switch has delivered 100% uptime across their facilities. At Switch, every team member is driven to produce real results for their clients – technologically and financially. Switch data center ecosystems empower their clients with numerous options for innovation, economies of scale, risk mitigation, sustainability, and investment protection.

Company Profile

Switch's advanced data centers are the center of their platform and provide power densities that exceed industry averages with efficient cooling, while being powered by 100% renewable energy. Two of the Switch data centers are the only carrier-neutral colocation facilities in the world to be certified Tier IV Design, Tier IV Facility, and Tier IV Gold in Operational Excellence. While these certifications have been the highest classifications available in the industry, Switch is building their current facilities to their proprietary Tier 5 Platinum standards, which exceed Tier IV standards. Switch's platform has powerful network effects and nurtures a technology ecosystem that benefits its participants. Switch continues to further enhance these benefits as they innovate and expand their platform ecosystem. Switch currently has over 1,000 customers, including technology and digital media companies, cloud, and managed service providers, financial institutions, and telecommunications providers.

The growing nexus between Internet connectivity, Internet-based services, data and analytics, and the advancement of computational processing power is rapidly expanding the amount of data that enterprises can access and manage. At the same time, the Internet of Everything is exponentially expanding the available data sources, as utility grids, automobiles, aircraft, home appliances, wearable devices, and numerous other sources are all connecting to the Internet. The compute capacity necessary to manage and analyze this data is also advancing and demanding increasing amounts of power to operate. Switch believes that traditional technology infrastructure is not capable of supporting the growing wave of mission critical data and increasingly powerful IT equipment.

Switch presently owns and operates four primary campus locations, called Primes, which encompass fourteen colocation facilities with an aggregate of over 5.3 million gross square feet (GSF) of space. These facilities have approximately 470 megawatts (MW) of power available to them. Primes consist of The Core Campus in Las Vegas, Nevada; The Citadel Campus near Reno, Nevada; The Pyramid Campus in Grand Rapids, Michigan; and The Keep Campus in Atlanta, Georgia. Primes are strategically located in geographies that combine a low risk of natural disaster, favorable tax policies for customers deploying computing infrastructure, and low latency connectivity to major metropolitan markets, such as Los Angeles, San Francisco, Silicon Valley, Chicago, New York, Northern Virginia, and Miami. As a result, customers in these metropolitan markets can access Switch's colocation facilities while reducing exposure to higher taxes, higher cost of power, and higher risk of natural disaster that might be prevalent in other markets. Switch can also use their Switch Modular Optimized Design (MOD) technology to build single-user facilities and are actively pursuing opportunities to deploy this technology in a build-to-suit offering for their enterprise customers.

As additional locations and sectors within the four existing Prime campus locations are opened for Colocation Services, the same / similar controls tested within this report are implemented / in place.

INFORMATION SECURITY PROGRAM

Description of Services Provided

Physical Security

Exterior Barriers

From well-defined perimeters consisting of signage, blast walls, and gates, to clear avenues of approach and backup perimeter barriers, the first layer of physical security is extensive. Exterior walls are constructed of either steel reinforced poured concrete or masonry reinforced beyond building code requirements. Entry points are kept to a minimum and each exterior door is reinforced, alarmed, access-controlled, and viewed by two dedicated fixed cameras.

Interior Barriers and Customer Compartmentalization

Exterior doors lead into specially engineered mantraps built over fire corridor wall construction. The mantraps are sheeted with steel and seams are strapped by aluminum. Access points off the mantrap require additional multi-factor biometric authentication of the card holder and are controlled via a 24 hour per day security officer and mantrap relay logic. Each mantrap includes fixed cameras viewing each door.

Each customer space, whether it is a cage, cabinet, or suite, is individually locked, protected, and monitored. Additional security safeguards, such as mantraps, intrusion sensors, and surveillance cameras, can be added to these spaces at the customer's request.

Positive Access Control

Positive Access Control is the application of a two-fold access principle stemming from the questions, "Who are you? And why should we let you in?" When first granted access to the facility, a multi-step process is in place to determine identity and verify need for access. In addition to the metal walls, turnstiles, cameras, intercoms, and biometric readers, Switch's access control takes on further hardening by the Positive Access Control procedures deployed at the facilities. Positive Access Control requires that a proprietary 24 hours per day officer staffed security command center (SECOM) verifies that the person standing in the mantrap matches a file photo. After confirmation, the officer activates the second proximity and biometric reader for use.

The access process is further continued with periodic access audits performed each shift by the shift supervisor. Customer audits are conducted monthly by the campus security manager. A complete audit of personnel with access to the facilities is conducted by the Security Director on a semi-annual basis.

Surveillance

Surveillance equipment for the facilities follows an elite standard set by a board-certified security professional. Fixed cameras are high-resolution color (520 lines) or digital high definition (HD) with automatic low light switching, capable of viewing up to 0.1 lux. Pan / tilt / zoom (PTZ) cameras are used on the exterior and areas of sensitivity. Video is digitally recorded at common interchange format (CIF) resolution at 15 images per second (IPS) upon motion at 4CIF 30 IPS upon operator command or at select zones requiring enhanced video. Video is retained for 100 +/- 10 days.

Switch deploys active surveillance with on-staff officers operating the camera system 24 hours per day. Camera operators use the Identify, Observe and Understand (IOU) methodology. The IOU methodology includes constant monitoring, use of cameras for detection, and a usable video product for investigations.

Sensors

Detectors are used around the property and provide early warning for perimeter and sensitive area intrusion. Sensor types include infrared motion, ultrasonic motion, photoelectric motion, electromechanical, internal lock, and seismic. These sensors are installed based on the environment or protection needs.

Security Team

Switch has a proprietary SECOM fully staffed 24 hours per day. Security staff members are hired with military and law enforcement security experience and must complete an extensive training period, which includes security system instruction, procedure and policy instruction, and non-lethal weapon training. The Security Academy was developed in accordance with the current American Society for Industrial Security (ASIS) International Guideline on Private Security Officer Selection and Training (ASIS GDL PSO-2010) and the 90-day field training officer (FTO) program. A security supervisor oversees each shift and reports to the campus security manager. Security supervisors are required to attend a Security Management course, and officers in management positions are required to be active members of ASIS International.

Please refer to the following link for related pictures and detailed information: http://www.switch.com.

Infrastructure Operations (Environmental Security)

Switch employs the latest advanced environmental controls to protect the systems of its customers as well as operating with energy efficiency. These systems are managed and monitored by the Data Center Operations (DCO) and Energy Management Systems (EMS) teams.

Fire Protection

Fire protection includes fire, smoke, and heat detection monitored 24 hours per day. Sensors are located throughout the data centers and provide alerts to physical security personnel and a third-party monitoring company for response. Data center areas are protected by aspirating smoke detectors, which are programmed to identify smoke in the incipit stage.

The data centers are equipped with dual-interlock pre-action dry pipe sprinklers. Specifically, these dual-interlock pre-action sprinklers require both a smoke detection event and the activation of sprinklers to release water into the pipes. This allows for quick response to a fire with a lower risk of water damage in the case of a smaller fire or false alarm.

Heating, Ventilation, and Cooling (HVAC)

Switch utilizes advanced, patented techniques starting with a custom-designed thermal separate compartment in facility or (t-scif) air-flow system. This airflow system pulls the warm air away from customer systems into a separate compartment. The warm air is taken out of the core SUPERNAP facility designed for 74 high-grade Switch-designed and patented TSC-600 and TSC-1000 HVAC units which are physically adjacent to the data center, each containing six types of air conditioning systems. Within the data centers, areas where warm or hot air travels are marked in red.

Please refer to the following link for related pictures and detailed information: http://www.switch.com.

Power Management

Switch utilizes multiple in-bound connections from electricity providers. Tri-redundant power systems, which balance dual in-bound power connections across three sources of power, optimize the power utilization. Power is currently provided in redundancy through the use of uninterruptable power supply (UPS) devices which are fed by generators across the campuses. Power distribution units are managed and secured to prevent tampering. Power cabling within the data center is color-coded for quick and succinct identification of circuits and to assist with troubleshooting.

Please refer to the following link for related pictures and detailed information: http://www.switch.com.

Support for Colocation Services

Switch maintains dedicated support for its customers 24 hours per day via the Network Operations Center (NOC). NOC and engineering staff are available to assist with network troubleshooting and provide "hands-on" services to support customers.

NOC representatives follow defined procedures to facilitate confirmation of identification, customer communication of unexpected events that may impact their systems, customer authorization (only authorized customer representatives can open a service request), and functional escalation for customer service requests and incidents.

NOC representatives monitor customer inquiries, support issues, and incidents on a real-time basis. Issues are documented in the Living Data Center (LDC) ticketing system and tracked to resolution.

The ticketing system / customer relationship management (CRM) system contains a complete purchased product hierarchy, installed equipment, and the physical and logical infrastructure layouts of individual customer solutions. The complete history of customer service requests and incidents are recorded in the ticketing system. Customer-specific information is handled confidentially through permission-access levels in the ticketing system and access to customer infrastructures. Documented procedures are in place for the monitoring of customer support operations. Furthermore, volume analysis, response times, and procedural adherence are monitored to help ensure customer obligations are met.

Network Management and Monitoring (Logical Security)

Since Switch has no logical access to any customer's equipment or data, each customer is responsible for its own network security. Switch manages the network connectivity to the Internet via its multiple providers. Switch's core routers are managed by the network engineering team and monitored by the NOC 24 hours per day. Routers are configured for high availability in active-active mode such that if one fails or connectivity is lost, network traffic is diverted accordingly.

Scope Definition

The scope of this engagement includes Switch's colocation services performed at the following facilities:

Name	Address
Las Vegas 2 (LAS 2)	2475 Arden St, Las Vegas, NV 89104
Las Vegas 4 (LAS 4)	4495 East Sahara Ave, Las Vegas, NV 89104
Las Vegas 5 (LAS 5)	4489 East Sahara Ave, Las Vegas, NV 89104
Las Vegas 7 (LAS 7)	7135 South Decatur Blvd, Las Vegas, NV 89118
Las Vegas 8 (LAS 8)	5225 West Capovilla Ave, Las Vegas, NV 89118
Las Vegas 9 (LAS 9)	7365 Lindell Rd, Las Vegas, NV 89139
Las Vegas 10 (LAS 10)	7375 Lindell Rd, Las Vegas, NV 89139
Las Vegas 11 (LAS 11)	7380 Lindell Rd, Las Vegas, NV 89118
Las Vegas 12 (LAS 12)	5325 West Capovilla Ave, Las Vegas, NV 89118
Las Vegas 15 (LAS 15)	5660 Badura Ave, Las Vegas, NV 89118
Reno 1 (RNO 1)	1 Superloop Circle, McCarran, NV 89437
Reno 2 (RNO 2)	2 Superloop Circle, McCarran, NV 89437
Grand Rapids 1 (GRR 1)	6100 East Paris Ave, Grand Rapids, MI 49512
Atlanta 1 (ATL 1)	1 Switch Way, Lithia Springs, GA 30122

Description of Electronic Protected Health Information (ePHI) Data Flows

Switch operates colocation facilities whereby their customers rent space for their systems and connectivity to the broader Internet. Switch personnel maintain physical access to infrastructure containing ePHI data; however, logical access to systems and data is the full responsibility of the customer. Switch provides secure space, power, and environmental controls for customers, some of which fall under Health Insurance Portability and Accountability Act (HIPAA) compliance.

Security Program Description

Infrastructure and Software

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

Primary Infrastructure			
Production System	**Business Function Description**	**Operating System Platform**	**Physical Location**
The Living Data Center (LDC) Application	Overall environmental conditions monitoring as well as ticketing system capability to track incidents and resolutions.	Linux	Las Vegas, Nevada Reno, Nevada Grand Rapids, Michigan Atlanta, Georgia
Microsoft Active Directory Domain	Network domain supporting internal systems applicable to the Colocation Services.	Windows	
Cisco Border and Private Routers	Network devices in place to direct traffic and filter unauthorized inbound network traffic from the Internet.	Cisco Internetwork Operating System (IOS)	
Honeywell Badge Access System	Physical access control supporting the Colocation Services at the Las Vegas, Reno, and Grand Rapids facilities that was decommissioned during November 2022. The in-scope facilities using Honeywell transitioned to C-Cure prior to the end of November 2022.	Windows	
C-Cure Badge Access System	Physical access control supporting the Colocation Services at the Las Vegas, Reno, Grand Rapids, and Atlanta facilities.		

In addition, Switch utilizes CrowdStrike antivirus software for antivirus protection for the Windows production servers and workstations. Furthermore, Switch utilizes Milestone Video Management System (VMS) for managing the security cameras for the interior and exterior of the data centers.

People

Switch utilizes specific functional areas of operations that support the scope of this review that include, but are not limited to, the following:

- Executive Management – responsible for overseeing company-wide activities, establishing and accomplishing goals, and overseeing objectives.
- Security Operations (SecOps) department – responsible for monitoring and protecting the facility from unauthorized access, damage, and interference.
- Network Operations (NetOps) department – responsible for implementation of product development and optimization, client implementation, and technical operations.
- Data Center Operations (DCO) – responsible for monitoring and maintaining critical infrastructure including electrical and cooling infrastructure. Also responsible for preparing customer environment (cage, cabinet) and performing everyday maintenance of the facility.
- Energy Management Systems (EMS) department – responsible for monitoring and maintaining critical infrastructure including power equipment and infrastructure.
- Network Engineering department – responsible for managing network architecture.
- Facilities Services department – responsible for providing user entities with assistance before and after the initial sale by providing information, guidance, and continued support.

- Human Resources (HR) department – responsible for HR policies, practices, and processes with a focus on key HR department delivery areas (e.g., talent acquisitions, employee retention, compensation, employee benefits, performance management, employee relations, development, and employee-related incidents and investigations).
- Legal department – responsible for legal and regulatory issues involving corporate risk and corporate compliance.

Security Awareness Training

A security awareness training program is established that includes the following components:

- New employees, customers, and vendors are required to sign a completed security orientation policy acknowledgment.
- Relevant personnel are directed by the EVP of SecOps to regularly undergo internal training courses.
- Security personnel maintain subscriptions to outside sources for notifications of threats or vulnerabilities within the industry.
- Security personnel meet on a weekly basis to discuss security metrics and any identified threats and vulnerabilities as a component of security awareness.
- Employees are required to take a Security Awareness Training and acknowledge / sign the Information Security Policy annually.

Access, Authentication, and Authorization

In order to gain access to the firewalls and routers, a user must authenticate with a user account and password via a secure shell (SSH) program to help ensure that the sessions are encrypted. The routers may only be managed from an internal network as SSH is not running on the public portion of the routers. SSH sessions are programmed to terminate a session after a predefined period of inactivity.

The network engineering team manages the security administration of the firewalls and routers and is required to authenticate through a terminal access controller access-control system plus (TACACS+) server which allows for individualized user account access, administration, and logging. These unique user accounts are defined by the TACACS+ server and are configured to authenticate using the corporate network domain.

The network domain is configured to enforce password requirements that include minimum length, expiration intervals, complexity, minimum history, and invalid account lockout threshold. Additionally, the operating system and badge access system are also configured to inherit credentials from the corporate network domain. Encrypted VPNs are required for remote access to production and enforce two-factor authentication.

Predefined access groups are employed within the network domain, operating system, badge access system, VPN system, and centralized authentication system to limit access based on job responsibilities. Additionally, administrator access to the aforementioned systems is restricted to only those personnel responsible for those activities via user account permissions and group assignments. Management reviews employee access privileges on a semi-annual basis.

IT management has configured the network domain, operating system, badge access system, VPN system, firewalls, and centralized authentication system to log access related events. IT management reviews these logs on an ad hoc basis to determine if any suspicious or unauthorized activity has occurred.

Access Requests and Access Revocation

Upon hire, an employee's production system access is requested, communicated, and approved by the employee's manager. The system access request details the specific production systems and required levels of access privileges. When an employee ends their employment, a termination checklist is completed to document the offboarding procedures performed and production system access is revoked.

Physical Security

Switch has implemented various physical security protocols to protect the business premises and information systems from unauthorized access. A badge access system is in place 24 hours per day to control access to the office. Predefined access groups are utilized to provide access depending on the individual's role and responsibilities. Physical access to the data center is documented and approved by the employee's manager prior to access being granted, while physical access to customer cages is documented and approved by the customer prior to access being granted. Badge access attempts are logged by the system and are traceable to specific badge access cards. Management reviews employee and customer access privileges on a semi-annual basis. The ability to administer the badge access system is restricted to authorized security management personnel. If an individual who has physical access to the Switch facilities is terminated, security management personnel revoke the badge access privileges within 24 hours as a component of the termination process.

The building perimeters for the facilities include fences, walls, and entrance gates controlled by guards or card access. In addition, surveillance cameras are utilized by security personnel to monitor the main entrance to the facilities in order to identify visitors and contractors prior to granting access to the facilities. Visitors must present photo identification before being granted access to the facilities. Personnel at the facilities are distinguished as being an employee, customer, or contractor with a functioning color-coded badge access card or a visitor with a non-functioning visitor badge. Prior to being granted access to the secure interior of the data centers, personnel and authorized customers must enter a mantrap where they must scan the badge access card and provide biometric credentials. Personnel and authorized visitors are required to provide badge access cards and biometric identification for both entry and exit of interior doors. Visitors without badge access cards are required to be escorted by authorized employees while within the facilities.

Switch maintains and monitors activity logs of certain physical movements within the facilities on an as needed basis. Physical movements captured and monitored include date / time, event, badge access card details, and device. Digital surveillance cameras are in place to monitor the facility entrances, the building perimeters, and other areas within the facilities. Video surveillance captured by the camera system is archived allowing the capability for review as needed. The facilities are monitored 24 hours per day by security personnel with the use of motion-sensitive digital surveillance cameras, alarms, and motion detectors. The physical security hardware (e.g., monitoring servers, DVRs) is secured behind locked server racks and physical cages. An incident reporting system is utilized by security personnel to document any physical security incidents.

Environmental Security

Switch has implemented various environmental security protocols to protect the business premises and information systems from potential environmental issues. The Switch facilities are protected by fire detection and suppression equipment that includes fire alarms, dry-pipe water sprinklers, fire and smoke detectors, hand-held fire extinguishers, and smoke and heat sensors. On a quarterly basis, the fire detection and suppression equipment undergo an inspection from a third-party specialist to help ensure that the equipment is in proper working order. Hand-held fire extinguishers undergo maintenance inspections on an annual basis.

Management utilizes an environmental monitoring tool which is configured to systematically monitor the humidity and temperature levels within the Switch data centers. The system is configured to automatically send e-mail notifications to operations personnel when predefined thresholds are exceeded. An inspection matrix guides the frequency of inspection for critical infrastructure including power and cooling systems.

The data centers are designed to optimize cool air flow and utilize redundant air conditioning units to keep infrastructure equipment at optimal temperatures. On a quarterly basis, the air conditioning systems undergo an inspection from a third-party specialist to help ensure that the equipment is in proper working order. The facilities are equipped with multiple UPS systems and diesel generators to provide electricity in the event of a power outage. The data centers also contain two distinct electrical connections to the electrical company's substation. Utility power is run through the UPS battery systems so that customers receive clean, conditioned battery power. In the event that a loss of utility power occurs, the generators will engage and begin supplying power to the UPS systems. Whether it is from utility or generator power, each customer draws power from the UPS battery systems, ensuring smooth transitions from utility to generator and back again. On a semi-annual basis, UPS inspections are performed, and on a quarterly basis, generator inspections are performed to help ensure that the systems are in proper working order. Additionally, internal personnel perform preventative maintenance procedures on the UPS systems and generators on a quarterly basis.

Malicious Software Management

Windows production servers and workstations are configured with CrowdStrike antivirus software which is configured to scan for updates to antivirus definitions and update signatures on a real-time basis and has on-access scanning of executables and files.

HR Policies and Practices

Switch's HR policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities. Specific control activities that Switch has implemented in this area are described below:

- **Management has established pre-hire screening procedures which are performed for employee candidates.**
- **New hire onboarding includes, but is not limited to, the following elements:**
    - **Verification that the employee has signed the employee agreement;**
    - **Verification that the employee has signed the confidentiality agreement;**
    - **Verification that the employee has signed an acknowledgment of receipt of employee handbook document; and**
    - **Verification that the employee has taken security training and signed an acknowledgment of such training.**
- Management utilizes termination procedures which include, but are not limited to, the following elements:
    - Collection of company property;
    - Revocation of physical and system access rights; and
    - Signatures of each person that performs requisite tasks.
- Evaluations are performed for employees on an annual basis.

Disaster Recovery

Business resiliency plans, including disaster recovery plans, and contingency plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event. The plans include roles and responsibilities, recovery time objectives (RTO), procedures for various scenarios, and task checklists in the event of an emergency. Additionally, disaster recovery tests are performed on an annual basis. The results of the annual disaster plan are recorded and tracked to identify and monitor potential threats to the critical infrastructure supporting the Colocation Services.

Ongoing Monitoring

The entity's IT security group monitors the security impact of emerging technologies, and the impact of applicable laws or regulations are considered by senior management. Ongoing monitoring consists of IT personnel receiving e-mail notifications and subscriptions, as well as following blogs to stay informed of the latest IT trends which could affect system security and availability. IT security personnel utilize a third-party utility to perform a vulnerability scan of the production servers on a monthly basis to identify threats and assess their potential impact to the production environment. Any security vulnerabilities that are identified are triaged by IT security personnel and monitored through resolution.

Capacity and Availability Monitoring

Switch has implemented an internally developed custom built application called SYSLOG to monitor the network devices' capacity and availability levels (e.g., central processing unit (CPU) levels, uptime, etc.) and alert operations personnel when predefined thresholds have been met. Switch uses an enterprise monitoring tool to log and monitor network availability and security incidents.

On-call personnel are notified via e-mail by SYSLOG of availability issues that exceed predefined thresholds on monitored network devices. The NOC is staffed on a 24 hour a day on-call basis to respond to availability issues. Additionally, operations meetings are held on a weekly basis to review availability trends and availability forecasts as compared to system commitments.

Incident Response

The network infrastructure is monitored 24 hours per day by NOC technicians to assist with network issues and to respond to customer inquiries and incidents. Management has implemented procedures to guide NOC technicians in identifying and responding to network related incidents, as well as incident response and escalation procedures in the event that an event is detected, to provide timely and consistent communication to the business and customers.

A proprietary ticketing system, LDC, was developed and is utilized to handle network related issues in order to manage, track, and respond to network issues until resolution. When an issue is detected, NOC technicians will examine the issue and create a ticket to assign priority level on a scale (1-5) based on the urgency and impact of the incident to the business and/or the customer, and to determine predefined timelines to resolve the issue. If the ticket is not responded to within a predefined timeline based on its severity, the ticketing system is configured to notify NOC technicians of the open ticket until the ticket is addressed. Incidents identified by customers can be communicated to the NOC by phone, e-mail, or on the LDC portal.

If the issue cannot be resolved within the predefined timeline, escalation procedures have been implemented for the assigned NOC technician to notify the responsible department and/or vendor through a predetermined set of contacts. Once the affected departments have been notified of the issue, e-mail updates are sent out to the business or customers on an as needed basis until the issue is resolved. Once the issue is fixed, the NOC technician will update the support ticket with full details of the issue resolution and close the ticket. Additionally, management meetings are held on a biweekly basis to discuss incidents and corrective measures to help ensure that incidents are resolved.

Third-Party Services and Monitoring

Switch does not have access to data residing on colocation or network customer IT equipment and therefore cannot and does not share that data with any third parties, vendors, or contractors. For third parties utilized for internal services, Switch maintains documented vendor management policies to address the following:

- Access control for a vendor or business partner
- Due diligence process prior to accepting new vendors or business partners
- Monitoring process to review vendor and business partner compliance on a periodic basis
- Termination of contract

Switch monitors threats arising from the use of vendors and third parties as part of the risk assessment process on an annual basis.

Breach Notification Description

Documented breach notification policies and procedures are in place to guide personnel in notifying a customer following the discovery of a breach of unsecured protected health information (PHI). The policies require Switch to identify each individual whose unsecured PHI was, or is reasonably believed to have been accessed, acquired, used, or disclosed during the breach. Additionally, Switch does not process, subprocess, access, transmit, receive, manage, maintain, or in any way interact with client data on customer equipment.

The elements required to be included within the notification include, but are not limited to, the following:

- Description of what happened (including the date of the breach and discovery).
- Description of the types of unsecured protected health information that were involved in the breach.
- Steps the individual should take to protect themselves from potential harm resulting from the breach.
- Description of what is being done to investigate the breach, to mitigate harm to individuals, and to protect against further breaches.

RISK ASSESSMENT

Risk Assessment Scoping

Security and risk management are of primary importance to Switch. Switch's management has placed into operation a risk assessment process to identify and manage risks that could affect the organization's ability to provide reliable Colocation Services for user entities. This process requires management to identify significant risks in their areas of responsibility and to implement sufficient measures to address those risks.

Switch faces a variety of risks from external and internal sources, and a precondition to Switch's risk assessment methodology is the establishment of objectives, linked at different levels and internally consistent. Objectives are set at the strategic level, establishing a basis for operations, reporting, and compliance objectives. Objectives are aligned with Switch's risk appetite, which drives risk tolerance levels.

More specific objectives flow from the entity's broad strategy. Entity-level objectives are linked and integrated with more specific objectives established for various "activities," such as sales, marketing, and operations, making sure they are consistent. These sub-objectives, or activity-level objectives, include establishing goals and may deal with product line, market, financing, and profit objectives.

By setting objectives at the entity and activity levels, Switch can identify success factors. Success factors exist for the entity, a business unit, a function, a department, or an individual. Objective setting enables management to identify measurement criteria for performance, with focus on success factors. Switch has established certain broad categories including:

- Operations objectives – these pertain to effectiveness and efficiency of the operations, including performance and delivery goals and safeguarding resources against loss. They vary based on management's choices about structure and performance.
- Compliance objectives – these objectives pertain to adherence to laws and regulations to which Switch and their customers are subject. They are dependent on external factors, such as government and industry regulation.

Regardless of whether an objective is stated or implied, Switch's risk assessment process considers risks that may occur. Switch has considered significant interactions between itself and relevant external parties and risks that could affect the organization's ability to provide reliable service to its user entities.

Potential Threats, Vulnerabilities, and Current Security Measures

Switch's management has placed into operation a risk assessment process in its overall Cyber Security Program Plan (CSPP) that adopts elements of the Argonne vulnerability index (VI) process and the Department of Homeland Security (DHS) Infrastructure Survey Tool (IST). The IST is a web-based risk assessment dashboard that calculates Switch's overall risk profile based on questionnaires completed by management and the risks identified and controls implemented in the following areas:

- Robustness
- Resourcefulness
- Redundancy

Switch's IST-based risk assessment process includes identifying threats to the six vulnerability components and 42 subcomponents of Switch's infrastructure. The six major vulnerability components of Switch's Colocation Services include the following:

- Physical security
- Security management
- Security force
- Information sharing
- Protective measure assessment
- Dependencies

Each of the six major IST vulnerability components is correlated with protective measures and vulnerabilities that may impact the component. During the assessment, both the protective measure attributes and vulnerability attributes are assigned values. The weighted sum of these values creates a protective measure index (PMI) and a VI. These indices are used to determine the strength of Switch's risk profile against industry competitors and provide a standardized method for assessing risks and determining the most cost-effective remediation methods.

Likelihood / Impact Analysis

Switch's methodology for analyzing risks varies largely because many risks are difficult to quantify. Nonetheless, the process usually includes:

- Estimating the significance of a risk
- Assessing the likelihood (or frequency) of the risk occurring
- Considering how the risk should be managed (i.e., an assessment of what actions need to be taken)

Risk analysis includes identification of key business processes where potential exposures of some consequence exist. Once the significance and likelihood of risk have been assessed, management considers how the risk should be managed. This involves judgment based on assumptions about the risk, and reasonable analysis of costs associated with reducing the level of risk.

Necessary actions are taken to reduce the significance or likelihood of the risk occurring.

Risk Level Determination / Documentation

As part of the risk assessment, Switch assigns a risk level to each identified risk. When assigning an impact level, Switch considers two major factors that generally drive an organization's level of potential impact: the consequences of a security incident and political sensitivities.

Switch has defined the following impact levels when assigning risk levels:

- Low – limited adverse effect on the organization or individuals and may noticeably reduce the effectiveness for the organization to perform its primary functions.
- Moderate – serious adverse effect on the organization or individuals and may significantly reduce the effectiveness for the organization to perform its primary functions.
- High – severe or catastrophic adverse effect on the organization or individuals and may cause the organization the inability to perform one or more of its primary functions.

Risk Management Program Monitoring and Maintenance

Switch has implemented a process to remediate any issues found during periodic testing and evaluations. Facility and security management meet on at least a semi-annual basis to discuss the progress of remediation for any issues found. These issue remediation events are documented in a plan of action and milestones which are updated and reviewed on a semi-annual basis by management to determine status of control implementation projects to mitigate gaps.

APPLICABLE CRITERIA

Switch management has made the determination regarding the applicability of the established performance criteria as it pertains to the in-scope services (the "applicable criteria"). Switch asserts that it is not a Business Associate as defined in 45 CFR 160.103, et. seq., as amended. Switch does not access, manage, maintain, transmit, receive,

process, subprocess, or otherwise interact with customer data. As such, it would not meet the qualification of "where the provision of the service involves the disclosure of protected health information from such covered entity" to Switch. Rather, Switch provides physical space and associated physical and environmental controls but does not engage in logical access of customer data. For additional information regarding Switch's policies, please visit www.switch.com/aup.

The table below provides the regulation references (section) and key activity, which relate to the established performance criteria, that Switch management has asserted to be in-scope for the purposes of this attestation:

Section	Key Activity	Applicable Criteria	
		Yes	No
	Security		
§164.306(a)	General Requirements	✓	
§164.306(b)	Flexibility of Approach	✓	
§164.308(a)	Security Management Process	✓	
§164.308(a)(1)(ii)(A)	Security Management Process – Risk Analysis	✓	
§164.308(a)(1)(ii)(B)	Security Management Process – Risk Management	✓	
§164.308(a)(1)(ii)(C)	Security Management Process – Sanction Policy	✓	
§164.308(a)(1)(ii)(D)	Security Management Process – Information System Activity Review		✓
§164.308(a)(2)	Assigned Security Responsibility	✓	
§164.308(a)(3)(i)	Workforce Security	✓	
§164.308(a)(3)(ii)(A)	Workforce Security – Authorization and/or Supervision	✓	
§164.308(a)(3)(ii)(B)	Workforce Security – Workforce Clearance Procedure	✓	
§164.308(a)(3)(ii)(C)	Workforce Security – Establish Termination Procedures	✓	
§164.308(a)(4)(i)	Information Access Management	✓	
§164.308(a)(4)(ii)(A)	Information Access Management – Isolating Healthcare Clearinghouse Functions		✓
§164.308(a)(4)(ii)(B)	Information Access Management – Access Authorization	✓	
§164.308(a)(4)(ii)(C)	Information Access Management – Access Establishment and Modification	✓	
§164.308(a)(5)(i)	Security Awareness and Training	✓	
§164.308(a)(5)(ii)(A)	Security Awareness and Training – Security Reminders	✓	
§164.308(a)(5)(ii)(B)	Security Awareness, Training, and Tools – Protection from Malicious Software		✓
§164.308(a)(5)(ii)(C)	Security Awareness, Training, and Tools – Log-in Monitoring		✓
§164.308(a)(5)(ii)(D)	Security Awareness, Training, and Tools – Password Management		✓
§164.308(a)(6)(i)	Security Incident Procedures	✓	

Section	Key Activity	Applicable Criteria	
		Yes	No
§164.308(a)(6)(ii)	Security Incident Procedures – Response and Reporting	✓	
§164.308(a)(7)(i)	Contingency Plan	✓	
§164.308(a)(7)(ii)(A)	Contingency Plan – Data Backup Plan		✓
§164.308(a)(7)(ii)(B)	Contingency Plan – Disaster Recovery Plan		✓
§164.308(a)(7)(ii)(C)	Contingency Plan – Emergency Mode Operation Plan	✓	
§164.308(a)(7)(ii)(D)	Contingency Plan – Testing and Revision Procedure	✓	
§164.308(a)(7)(ii)(E)	Applications and Data Criticality Analysis		✓
§164.308(a)(8)	Evaluation of Analysis	✓	
§164.308(b)(1)	Business Associate Contracts and Other Arrangements		✓
§164.308(b)(2)	Assigned Security Responsibility		✓
§164.308(b)(3)	Business Associate Contracts and Other Arrangements – Written Contract or Other Arrangement		✓
§164.310(a)(1)	Facility Access Controls	✓	
§164.310(a)(2)(i)	Facility Access Controls – Contingency Operations	✓	
§164.310(a)(2)(ii)	Facility Access Controls – Facility Security Plan	✓	
§164.310(a)(2)(iii)	Facility Access Controls – Access Control and Validation Procedures	✓	
§164.310(a)(2)(iv)	Facility Access Controls – Maintain Maintenance Records	✓	
§164.310(b)	Workstation Use		✓
§164.310(c)	Workstation Security		✓
§164.310(d)(1)	Device and Media Controls		✓
§164.310(d)(2)(i)	Device and Media Controls – Disposal		✓
§164.310(d)(2)(ii)	Device and Media Controls – Media Re-use		✓
§164.310(d)(2)(iii)	Device and Media Controls – Accountability		✓
§164.310(d)(2)(iv)	Device and Media Controls – Data Backup and Storage Procedures		✓
§164.312(a)(1)	Access Control		✓
§164.312(a)(2)(i)	Access Control – Unique User Identification		✓
§164.312(a)(2)(ii)	Access Control – Emergency Access Procedure		✓
§164.312(a)(2)(iii)	Access Control – Automatic Logoff		✓
§164.312(a)(2)(iv)	Access Control – Encryption and Decryption		✓
§164.312(b)	Audit Controls		✓
§164.312(c)(1)	Integrity		✓
§164.312(c)(2)	Integrity – Mechanism to Authenticate ePHI		✓

Section	Key Activity	Applicable Criteria	
		Yes	No
§164.312(d)	Person or Entity Authentication		✓
§164.312(e)(1)	Transmission		✓
§164.312(e)(2)(i)	Transmission Security – Integrity Controls		✓
§164.312(e)(2)(ii)	Transmission Security – Encryption		✓
§164.314(a)(1)	Business Associate Contracts or Other Arrangements	✓	
§164.314(a)(2)(i)(A)	Business Associate Contracts	✓	
§164.314(a)(2)(i)(B)	Business Associate Contracts	✓	
§164.314(a)(2)(i)(C)	Business Associate Contracts	✓	
§164.314(a)(2)(ii)	Other Arrangements	✓	
§164.314(a)(2)(iii)	Business Associate Contracts with Subcontractors	✓	
§164.314(a)(b)(1)	Requirements for Group Health Plans		✓
§164.314(b)(2)(i)	Group Health Plan Implementation Specification		✓
§164.314(b)(2)(ii)	Group Health Plan Implementation Specification		✓
§164.314(b)(2)(iii)	Group Health Plan Implementation Specification		✓
§164.314(b)(2)(iv)	Group Health Plan Implementation Specification		✓
§164.316(a)	Policies and Procedures	✓	
§164.316(b)(1)	Documentation	✓	
§164.316(b)(2)(i)	Documentation	✓	
§164.316(b)(2)(ii)	Documentation	✓	
§164.316(b)(2)(iii)	Documentation	✓	
	Breach Notification		
§164.414(a)	Administrative Requirements		✓
§164.530(b)	Training	✓	
§164.530(d)	Complaints		✓
§164.530(e)	Sanctions		✓
§164.530(g)	Refraining from Retaliatory Acts		✓
§164.530(h)	Waiver of Rights		✓
§164.530(i)	Policies and Procedures		✓
§164.530(j)	Documentation		✓
§164.402	Definitions: Breach – Risk Assessment, Breach Exceptions - Unsecured PHI	✓	
§164.404(a)(1)	Notice to Individuals		✓
§164.404(b)	Timeliness of Notification		✓
§164.404(c)(1)	Content of Notification		✓
§164.404(d)	Methods of Notification		✓
§164.406(a)	Notification to the Media		✓

Section	Key Activity	Applicable Criteria	
		Yes	No
§164.408	Notification to the Secretary		✓
§164.410	Notification by a Business Associate	✓	
§164.412	Law Enforcement Delay	✓	
§164.414(b)	Burden of Proof	✓	

The specific established performance criteria are detailed in the Results of Section 4 of this report.

It also provides the results related to the security and breach performance criteria as selected from the applicability table above.

SECTION 4

RESULTS

HIPAA SECURITY RULE

#	Control Activity	Results
§164.306(a): Covered entities and business associates must do the following:(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits. (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information. (3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part; and (4) Ensure compliance with this subpart by its workforce.		
1.01	Documented security policies and procedures are in place to guide personnel in practices and principles related to the HIPAA Security Rule.	No exceptions noted.
1.02	A ticketing system is utilized to document, track, and resolve reported security violations.	No exceptions noted.
§164.306(b): Flexibility of approach. (1) Covered entities and business associates may use any security measures that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart. (2) In deciding which security measures to use, a covered entity or business associate must take into account the following factors: (i) The size, complexity, and capabilities of the covered entity or business associate. (ii) The covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities. (iii) The costs of security measures. (iv) The probability and criticality of potential risks to electronic protected health information.		
1.03	Documented policies and procedures are in place to guide personnel in the assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of systems and infrastructure that may contain ePHI.	No exceptions noted.
1.04	A formal risk assessment is performed on at least an annual basis to assess the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI. Risks that are identified are rated using a risk evaluation process and are formally documented that includes, but is not limited to, the following factors: • Size, complexity, and capabilities • Technical infrastructure, hardware, and software security capabilities • Costs of security measures • Probability and criticality of potential risks to ePHI	No exceptions noted.
1.05	A ticketing system is utilized to document, track, and resolve reported security violations.	No exceptions noted.
§164.308(a): A covered entity or business associate must in accordance with 164.306: (1)(i) Implement policies and procedures to prevent, detect, contain, and correct security violations.		
1.06	Documented policies and procedures are in place to guide personnel in the assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of systems and infrastructure that may contain ePHI.	No exceptions noted.
1.07	Documented escalation / incident response procedures are in place to guide employees in reporting, acting upon, and resolving reported security violations.	No exceptions noted.
1.08	A ticketing system is utilized to document, track, and resolve reported security violations.	No exceptions noted.
§164.308(a)(1)(ii)(A): Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.		
1.09	Documented policies and procedures are in place to guide personnel in the assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI.	No exceptions noted.

#	Control Activity	Results
1.10	A formal risk assessment is performed on at least an annual basis to assess the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI. Risks that are identified are rated using a risk evaluation process and are formally documented that includes, but is not limited to, the following factors: • **Size, complexity, and capabilities** • **Technical infrastructure, hardware, and software security capabilities** • **Costs of security measures** • **Probability and criticality of potential risks to ePHI**	**No exceptions noted.**
§164.308(a)(1)(ii)(B): Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a).		
1.11	Documented policies and procedures are in place to guide personnel in the risk management process to reduce risks and vulnerabilities to a reasonable and appropriate level.	No exceptions noted.
1.12	Risks that are identified in the risk assessment are rated using a risk evaluation process and are formally documented, along with mitigation strategies, for management review.	No exceptions noted.
1.13	Employees sign an acknowledgment form upon hire indicating that they have been given access to the employee manual and electronic communications policy and understand their responsibility for adhering to the code of conduct outlined within the manual.	No exceptions noted.
1.14	Newly hired employees sign a written acknowledgment form documenting their receipt and understanding of the requirement to protect confidential information.	No exceptions noted.
1.15	Employees complete security awareness training on at least an annual basis to understand their obligations and responsibilities to comply with the corporate and business unit security policies.	No exceptions noted.
§164.308(a)(1)(ii)(C): Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.		
1.16	Documented sanction policies and procedures are in place for action to be taken when workforce members fail to comply with the security policies and procedures.	No exceptions noted.
1.17	Employees sign an acknowledgment form upon hire indicating that they have been given access to the employee manual and electronic communications policy and understand their responsibility for adhering to the code of conduct outlined within the manual.	No exceptions noted.
1.18	Sanctions are applied to workforce members when violations of the security policies and procedures are discovered.	No exceptions noted.
§164.308(a)(1)(ii)(D): Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.		
	Not applicable. Switch customers are responsible for logging and auditing of their own information system activity to meet this control requirement.	
§164.308(a)(2): Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.		
1.19	Responsibility of the development and implementation of information security policies and procedures is formally assigned to a Security Official and the responsibilities of the Security Official have been defined.	No exceptions noted.

#	Control Activity	Results
§164.308(a)(3)(i): Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.		
1.20	Documented policies and procedures are in place to guide personnel regarding access provisioning, modification, removal, and review.	No exceptions noted.
1.21	Management personnel perform user access reviews for the in-scope systems that may contain ePHI on a semi-annual basis to help ensure that access correlates with employee job functions and duties.	No exceptions noted.
§164.308(a)(3)(ii)(A): Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.		
1.22	Documented policies and procedures are in place to guide personnel regarding access provisioning, modification, removal, and review.	No exceptions noted.
1.23	Management personnel perform user access reviews for the in-scope systems that may contain ePHI on a semi-annual basis.	No exceptions noted.
1.24	Organizational charts are in place to communicate the defined key areas of authority, responsibility, and lines of reporting to personnel related to the design, development, implementation, operation, maintenance, and monitoring of systems that may contain ePHI. These charts are communicated to employees and updated as needed.	No exceptions noted.
§164.308(a)(3)(ii)(B): Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.		
1.25	Documented policies and procedures are in place to guide personnel regarding access provisioning, modification, removal, and review.	No exceptions noted.
1.26	Management personnel perform user access reviews for the in-scope systems that may contain ePHI on a semi-annual basis.	No exceptions noted.
1.27	Documented physical security policies and procedures are in place to guide personnel in physical security practices for secure areas.	No exceptions noted.
1.28	Background checks are performed for employees as a component of the hiring process.	No exceptions noted.
1.29	IT personnel revoke terminated employees' access to the in-scope systems as a component of the termination process.	No exceptions noted.
§164.308(a)(3)(ii)(C): Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(b).		
1.30	Documented policies and procedures are in place to guide personnel regarding access provisioning, modification, removal, and review.	No exceptions noted.
1.31	IT personnel revoke terminated employees' access to the in-scope systems as a component of the termination process.	No exceptions noted.
§164.308(a)(4)(i): Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.		
1.32	Documented policies and procedures are in place to guide personnel regarding access provisioning, modification, removal, and review.	No exceptions noted.
1.33	Management personnel perform user access reviews for the in-scope systems that may contain ePHI on a semi-annual basis to help ensure that access correlates with employee job functions and duties.	No exceptions noted.
§164.308(a)(4)(ii)(A): If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.		
	Not applicable. Switch is not a health care clearinghouse.	

#	Control Activity	Results
§164.308(a)(4)(ii)(B): Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.		
1.34	Documented policies and procedures are in place to guide personnel regarding access provisioning, modification, removal, and review.	No exceptions noted.
1.35	Department managers complete a new hire onboarding checklist prior to granting system access privileges to new employees.	No exceptions noted.
1.36	Management personnel perform user access reviews for the in-scope systems that may contain ePHI on a semi-annual basis.	No exceptions noted.
§164.308(a)(4)(ii)(C): Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.		
1.37	Documented policies and procedures are in place to guide personnel regarding access provisioning, modification, removal, and review.	No exceptions noted.
1.38	Department managers complete a new hire onboarding checklist prior to granting system access privileges to new employees.	No exceptions noted.
1.39	Management personnel perform user access reviews for the in-scope systems that may contain ePHI on a semi-annual basis.	No exceptions noted.
1.40	IT personnel revoke terminated employees' access to the in-scope systems as a component of the termination process.	No exceptions noted.
§164.308(a)(5)(i): Implement a security awareness and training program for all members of its workforce (including management).		
1.41	Policies and procedures regarding security awareness training are in place with elements that include, but are not limited to, the following: • How workforce members are provided the security awareness and training • Identifies workforce members (including managers, senior executives, and as appropriate, business associates, and contractors) who will be provided with the security and awareness training • How workforce members will be provided with security and awareness training when there is a change in the entity's information systems • How frequently security awareness and training will be provided to workforce members	No exceptions noted.
1.42	A formal security awareness training program is in place.	No exceptions noted.
1.43	Employees complete security awareness training on at least an annual basis to understand their obligations and responsibilities to comply with the corporate and business unit security policies.	No exceptions noted.
§164.308(a)(5)(ii)(A): Periodic security updates.		
1.44	The entity's IT security group monitors the security impact of emerging technologies, and the impact of applicable laws and regulations are considered by senior management.	No exceptions noted.
1.45	Employees complete security awareness training on at least an annual basis to understand their obligations and responsibilities to comply with the corporate and business unit security policies.	No exceptions noted.
1.46	Security reminders and updates are communicated to workforce members on an ongoing basis.	No exceptions noted.
§164.308(a)(5)(ii)(B): Procedures for guarding against, detecting, and reporting malicious software.		
	Not applicable. Switch customers are responsible for meeting this control requirement.	
§164.308(a)(5)(ii)(C): Procedures for monitoring log-in attempts and reporting discrepancies.		
	Not applicable. Switch customers are responsible for meeting this control requirement.	

#	Control Activity	Results
§164.308(a)(5)(ii)(D): Procedures for creating, changing, and safeguarding passwords.		
	Not applicable. Switch customers are responsible for meeting this control requirement.	
§164.308(a)(6)(i): Implement policies and procedures to address security incidents.		
1.47	Documented escalation procedures are in place to guide employees in the security incident response process that includes, but is not limited to, the following elements: • Identification of what specific event would be considered a security incident • Identification of workforce members' roles and responsibilities regarding security incidents • Management involvement regarding security incidents • Workforce members or roles to which the incident response policies and procedures are to be disseminated • Coordination of security incidents among business associates • Identifies what steps should be taken in response to a security incident • The frequency to review and update current security incident policies and procedures	No exceptions noted.
1.48	A ticketing system is utilized to manage, track, and respond to system and network problems and incidents.	No exceptions noted.
§164.308(a)(6)(ii): Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.		
1.49	Documented incident response procedures are in place to guide personnel that includes, but is not limited to, the following: • A methodology for defining security incidents based on levels of criticality • Provisions for reporting and responding to all types of known and suspicious security incidents based on criticality levels of such incidents • The roles and responsibilities of workforce members including the entity's security incident response team	No exceptions noted.
1.50	A ticketing system is utilized to manage, track, and respond to system and network problems and incidents.	No exceptions noted.
§164.308(a)(7)(i): Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.		
1.51	A business resiliency plan is in place to guide personnel in procedures to protect against disruptions caused by an unexpected event that includes, but is not limited to, the following: • Identification of workforce members' roles and responsibilities in the contingency process • Workforce members or roles to which the contingency policies and procedures are to be disseminated • Management involvement in contingency plans • Coordination of contingency processes among business associates • Identification of what steps should be taken in a contingency plan • The frequency to review and update current contingency policies and procedures • How frequently the contingency plan is tested	No exceptions noted.
1.52	Documented escalation procedures are in place to guide employees in reporting, acting upon, and resolving reported events.	No exceptions noted.

#	Control Activity	Results
§164.308(a)(7)(ii)(A): Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.		
	Not applicable. Switch customers are responsible for meeting this control requirement.	
§164.308(a)(7)(ii)(B): Establish (and implement as needed) procedures to restore any loss of data.		
	Not applicable. Switch customers are responsible for meeting this control requirement.	
§164.308(a)(7)(ii)(C): Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.		
1.53	A business resiliency plan is in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.	No exceptions noted.
§164.308(a)(7)(ii)(D): Implement procedures for periodic testing and revision of contingency plans.		
1.54	Documented policies and procedures are in place regarding contingency plans and their testing and revision that includes, but is not limited to, the following: • **Methods used to test the plan (component, system, or comprehensive)** • **Workforce members' roles and responsibilities in coordination of the test** • **How frequently tests will be conducted** • **How frequently contingency plans will be revised** • **Notification procedures**	**No exceptions noted.**
1.55	Disaster recovery plans are tested on at least an annual basis.	No exceptions noted.
1.56	Management personnel approve, review, and update the business resiliency plan on an annual basis.	No exceptions noted.
§164.308(a)(7)(ii)(E): Assess the relative criticality of specific applications and data in support of other contingency plan components.		
	Not applicable. Switch customers are responsible for meeting this control requirement.	
§164.308(a)(8): Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, which establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.		
1.57	A formal risk assessment is performed on at least 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.	No exceptions noted.
1.58	Internal vulnerability scans are performed on a monthly basis to identify potential infrastructure security vulnerabilities.	No exceptions noted.
1.59	A central antivirus server is configured with antivirus software to protect registered production Windows servers and workstations with the following configurations: • Scan for updates to antivirus definitions on a real-time basis • On-access scanning of executables and files	No exceptions noted.
§164.308(b)(1): A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with §164.314(a) that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.		
	Not applicable. Switch is not a covered entity and does not have access to customer data or share data with other providers.	
§164.308(b)(2): A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic protected health information on its behalf only if the business associate obtains satisfactory assurances, in accordance with §164.314(a), that the subcontractor will appropriately safeguard the information.		
	Not applicable. Switch is not a covered entity and does not have access to customer data or share data with other providers.	

#	Control Activity	Results
§164.308(b)(3): Document the satisfactory assurances required by paragraph (b)(1) or (b)(2) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of §164.314(a).		
	Not applicable. Switch is not a covered entity and does not have access to customer data or share data with other providers.	
§164.310(a)(1): Implement policies and procedures to limit physical access to Switch's electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.		
1.60	Physical access policies and procedures are in place for areas that may contain ePHI that includes, but is not limited to, the following: • **Workforce members' roles and responsibilities in facility access control procedures** • **Management involvement in the facility's access controls procedures** • **The process of how authorization credentials for facility access are issued** • **The process of removing workforce members' authorization credentials for physical access when such access is no longer required** • **Identification of how visitors' access is monitored** • **Methods for controlling and managing physical access devices** • **Facilities and areas that have physical access control implemented to safeguard ePHI**	**No exceptions noted.**
1.61	Physical access rights to the areas that may contain ePHI are reviewed on an annual basis to help ensure that physical access to data is restricted.	No exceptions noted.
1.62	IT personnel revoke terminated employee physical access rights upon notification of employee termination.	No exceptions noted.
1.63	Security personnel monitor access to the facilities' entrances and manage visitor access 24 hours per day.	No exceptions noted.
1.64	Personnel at the facilities are distinguished as being either an employee, customer, or contractor with a functioning color-coded badge access card or a visitor with a non-functioning visitor badge.	No exceptions noted.
1.65	Visitors are required to present a picture identification card, which is either retained or digitally scanned, and must be escorted by authorized individuals before being granted access to the facilities.	No exceptions noted.
1.66	A badge access system is in place to control access into and throughout the facility and data center.	No exceptions noted.
1.67	Security personnel assign access rights to employees for physical security zones through the use of predefined access groups.	No exceptions noted.
1.68	The data center utilizes a two-factor authentication system at the main entrance that requires an access code and badge access card credential for authorized entry into the data center.	No exceptions noted.
1.69	Access to physical areas that contain electronic information systems is restricted to badge access cards assigned to authorized personnel.	No exceptions noted.

#	Control Activity	Results
§164.310(a)(2)(i): Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.		
1.70	A physical security contingency plan is in place to guide personnel in procedures to protect against disruptions caused by an unexpected event with elements that include, but are not limited to, the following: • **Identification of who will need access to ePHI in the event of a disaster** • **Backup plan for access to the facility and/or ePHI** • **Workforce member roles and responsibilities from implementing the contingency plan for accessing ePHI in each department, unit, etc.** • **Procedures for accessing restored data at the alternate processing, storage, and work site** • **Procedures for the testing of contingency operations**	**No exceptions noted.**
1.71	The physical security and disaster recovery plans are tested on at least an annual basis.	No exceptions noted.
§164.310(a)(2)(ii): Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.		
1.72	A physical security plan is in place to guide personnel in procedures to protect against unauthorized physical access, tampering, or theft of ePHI with elements that include, but are not limited to, the following: • Identification of the physical security measures in place to provide physical security protection for facilities and equipment • Workforce members' roles and responsibilities regarding the facility security plan • Inventory of the entity's facilities that house equipment that create, maintain, receive, and transmit ePHI	**No exceptions noted.**
1.73	Physical access policies and procedures are in place for areas that may contain ePHI that includes, but is not limited to, the following: • Workforce members' roles and responsibilities in facility access control procedures • Management involvement in the facility's access controls procedures • The process of how authorization credentials for facility access are issued • The process of removing workforce members' authorization credentials for physical access when such access is no longer required • Identification of how visitors' access is monitored • Methods for controlling and managing physical access devices • Facilities and areas that have physical access control implemented to safeguard ePHI	No exceptions noted.
1.74	IT personnel revoke terminated employee physical access rights upon notification of employee termination.	No exceptions noted.
1.75	Security personnel monitor access to the facilities' entrances and manage visitor access 24 hours per day.	No exceptions noted.
1.76	Personnel at the facilities are distinguished as being either an employee, customer, or contractor with a functioning color-coded badge access card or a visitor with a non-functioning visitor badge.	No exceptions noted.
1.77	Visitors are required to present a picture identification card, which is either retained or digitally scanned, and must be escorted by authorized individuals before being granted access to the facilities.	No exceptions noted.
1.78	A badge access system is in place to control access into and throughout the facility and data center.	No exceptions noted.

#	Control Activity	Results
1.79	Security personnel assign access rights to employees for physical security zones through the use of predefined access groups.	No exceptions noted.
1.80	The data center utilizes a two-factor authentication system at the main entrance that requires an access code and badge access card credential for authorized entry into the data center.	No exceptions noted.
1.81	Access to physical areas that contain electronic information systems is restricted to badge access cards assigned to authorized personnel.	No exceptions noted.
§164.310(a)(2)(iii): Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.		
1.82	Physical access policies and procedures are in place for areas that may contain ePHI that includes, but is not limited to, the following: • **Workforce members' roles and responsibilities in facility access control procedures** • **Management involvement in the facility's access controls procedures** • **The process of how authorization credentials for facility access are issued** • **The process of removing workforce members' authorization credentials for physical access when such access is no longer required** • **Identification of how visitors' access is monitored** • **Methods for controlling and managing physical access devices** • **Facilities and areas that have physical access control implemented to safeguard ePHI**	**No exceptions noted.**
1.83	IT personnel revoke terminated employee physical access rights upon notification of employee termination.	No exceptions noted.
1.84	Security personnel monitor access to the facilities' entrances and manage visitor access 24 hours per day.	No exceptions noted.
1.85	Personnel at the facilities are distinguished as being either an employee, customer, or contractor with a functioning color-coded badge access card or a visitor with a non-functioning visitor badge.	No exceptions noted.
1.86	Visitors are required to present a picture identification card, which is either retained or digitally scanned, and must be escorted by authorized individuals before being granted access to the facilities.	No exceptions noted.
1.87	A badge access system is in place to control access into and throughout the facility and data center.	No exceptions noted.
1.88	Security personnel assign access rights to employees for physical security zones through the use of predefined access groups.	No exceptions noted.
1.89	The data center utilizes a two-factor authentication system at the main entrance that requires an access code and badge access card credential for authorized entry into the data center.	No exceptions noted.
1.90	Access to physical areas that contain electronic information systems is restricted to badge access cards assigned to authorized personnel.	No exceptions noted.
1.91	Security personnel utilize surveillance cameras to monitor the main entrance to the data centers and identify visitors and contractors prior to granting them access into the facilities.	No exceptions noted.
1.92	Digital surveillance video camera recordings are archived allowing capability for ad hoc investigations.	No exceptions noted.
§164.310(a)(2)(iv): Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).		
1.93	Security policies and procedures are documented to guide employee activities for granting, controlling, and monitoring physical access to the data centers.	No exceptions noted.

#	Control Activity	Results
1.94	A ticketing system is utilized to document and track repairs and modifications to physical security components within the facility.	No exceptions noted.
§164.310(b): Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.		
	Not applicable. Protected health information is not stored or processed on Switch workstations.	
§164.310(c): Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.		
	Not applicable. Protected health information is not stored or processed on Switch workstations.	
§164.310(d)(1): Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information, into and out of a facility, and the movement of these items within the facility.		
	Not applicable. Protected health information is not stored or processed on Switch workstations.	
§164.310(d)(2)(i): Implement policies and procedures to address the final disposition of electronic protected health information and/or the hardware or electronic media on which it is stored.		
	Not applicable. Device and media controls addressing the re-use of ePHI are the responsibility of Switch's customers.	
§164.310(d)(2)(ii): Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.		
	Not applicable. Device and media controls addressing the re-use of ePHI are the responsibility of Switch's customers.	
§164.310(d)(2)(iii): Maintain a record of the movements of hardware and electronic media and any person responsible therefore.		
	Not applicable. Maintenance of records of movements of hardware and electronic media are the responsibility of Switch's customers.	
§164.310(d)(2)(iv): Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.		
	Not applicable. Switch customers are responsible for configuring backup systems to backup ePHI.	
§164.312(a)(1): Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).		
	Not applicable. This control requirement is the responsibility of Switch customers.	
§164.312(a)(2)(i): Assign a unique name and/or number for identifying and tracking user identity.		
	Not applicable. This control requirement is the responsibility of Switch customers.	
§164.312(a)(2)(ii): Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.		
	Not applicable. This control requirement is the responsibility of Switch customers.	
§164.312(a)(2)(iii): Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.		
	Not applicable. This control requirement is the responsibility of Switch customers.	
§164.312(a)(2)(iv): Implement a mechanism to encrypt and decrypt electronic protected health information.		
	Not applicable. This control requirement is the responsibility of Switch customers.	
§164.312(b): Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.		
	Not applicable. This control requirement is the responsibility of Switch customers.	

#	Control Activity	Results
§164.312(c)(1): Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.		
	Not applicable. This control requirement is the responsibility of Switch customers.	
§164.312(c)(2): Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.		
	Not applicable. This control requirement is the responsibility of Switch customers.	
§164.312(d): Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.		
	Not applicable. This control requirement is the responsibility of Switch customers.	
§164.312(e)(1): Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.		
	Not applicable. This control requirement is the responsibility of Switch customers.	
§164.312(e)(2)(i): Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.		
	Not applicable. This control requirement is the responsibility of Switch customers.	
§164.312(e)(2)(ii): Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.		
	Not applicable. This control requirement is the responsibility of Switch customers.	
§164.314(a)(1): The contract or other arrangement between the covered entity and its business associate required by §164.308(b)(3) must meet the requirements of paragraph (a)(2)(i) or (a)(2)(ii) of this section, as applicable.		
1.95	Policies and procedures are in place to guide personnel in the selection and engagement with business associates or subcontractors who create, receive, maintain, or transmit ePHI.	No exceptions noted.
1.96	The entity requires that business associates and subcontractors sign a nondisclosure agreement and acknowledge the requirements for the confidentiality, integrity, and availability of ePHI.	No exceptions noted.
§164.314(a)(2)(i)(A): The contract must provide that the business associate will— (A) Comply with the applicable requirements of this subpart;		
1.97	Policies and procedures are in place to guide personnel in the selection and engagement with business associates or subcontractors who create, receive, maintain, or transmit ePHI.	No exceptions noted.
1.98	Customer service agreements are in place that require subcontractors to comply with security requirements of the system and notify management of suspected security incidents.	No exceptions noted.
1.99	Subcontractors attend a security orientation and sign an acknowledgment form agreeing to the requirements for the security of systems.	No exceptions noted.
§164.314(a)(2)(i)(B): The contract must provide that the business associate will, in accordance with §164.308(b)(2), ensure that any subcontractors that create, receive, maintain, or transmit electronic protected health information on behalf of the business associate agree to comply with the applicable requirements of this subpart by entering into a contract or other arrangement that complies with this section.		
1.100	Policies and procedures are in place to guide personnel in the selection and engagement with business associates or subcontractors who create, receive, maintain, or transmit ePHI.	No exceptions noted.
1.101	Customer service agreements are in place that require subcontractors to comply with security requirements of the system and notify management of suspected security incidents.	No exceptions noted.

#	Control Activity	Results
§164.314(a)(2)(i)(C): The contract must provide that the business associate will report to the covered entity any security incident of which it becomes aware, including breaches of unsecured protected health information as required by §164.410		
1.102	Customer service agreements are in place that require subcontractors to comply with security requirements of the system and notify management of suspected security incidents.	No exceptions noted.
1.103	Subcontractors attend a security orientation and sign an acknowledgment form agreeing to the requirements for the security of systems.	No exceptions noted.
§164.314(a)(2)(ii): The covered entity is in compliance with paragraph (a)(1) of this section if it has another arrangement in place that meets the requirements of §164.504(e)(3).		
1.104	Customer service agreements are in place that require subcontractors to comply with security requirements of the system and notify management of suspected security incidents.	No exceptions noted.
1.105	Subcontractors attend a security orientation and sign an acknowledgment form agreeing to the requirements for the security of systems.	No exceptions noted.
§164.314(a)(2)(iii): The requirements of paragraphs (a)(2)(i) and (a)(2)(ii) of this section apply to the contract or other arrangement between a business associate and a subcontractor required by §164.308(b)(4) in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.		
1.106	Customer service agreements are in place that require subcontractors to comply with security requirements of the system and notify management of suspected security incidents.	No exceptions noted.
1.107	Subcontractors sign agreements to acknowledge that requirements that apply to subcontractors in the same manner as requirements apply to contracts or other arrangements between a covered entity and business associate.	No exceptions noted.
§164.314(a)(b)(1): Except when the only electronic protected health information disclosed to a plan sponsor is disclosed pursuant to §164.504(f)(1)(ii) or (iii), or as authorized under §164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.		
	Not applicable. Switch is not a group health plan.	
§164.314(b)(2)(i): The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to– (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan.		
	Not applicable. Switch is not a group health plan.	
§164.314(b)(2)(ii): The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to– (ii) Ensure that the adequate separation required by §164.504(f)(2)(iii) is supported by reasonable and appropriate security measures.		
	Not applicable. Switch is not a group health plan.	
§164.314(b)(2)(iii): The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to– (iii) Ensure that any agent to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information.		
	Not applicable. Switch is not a group health plan.	
§164.314(b)(2)(iv): The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to– (iv) Report to the group health plan any security incident of which it becomes aware.		
	Not applicable. Switch is not a group health plan.	

#	Control Activity	Results
§164.316(a): Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in §164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity or business associate may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.		
1.108	Policies and procedures are in place to address specific policies and procedures needed to comply with the standards, implementation specification, or other requirements of the HIPAA Security Rule.	No exceptions noted.
§164.316(b)(1): (i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and(ii) If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record or the action, activity, or assessment.		
1.109	Policies and procedures are in place that address the entity maintaining written policies and procedures related to the security rule and written documents of (if any) actions, activities, or assessments required of the HIPAA Security Rule.	No exceptions noted.
§164.316(b)(2)(i): Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.		
1.110	Policies and procedures are in place that address required documentation being retained for six years from the date of its creation or the date when it last was in effect.	No exceptions noted.
§164.316(b)(2)(ii): Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.		
1.111	Policies and procedures are made available to the workforce members responsible for implementing the pertaining procedures via the company SharePoint.	No exceptions noted.
§164.316(b)(2)(iii): Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.		
1.112	Policies and procedures are in place that dictate the review and update of HIPAA Security Rule related policies and procedures on at least an annual basis.	No exceptions noted.

HITECH Breach Notification Rule

#	Control Activity	Results
§164.414(a): Administrative Requirements. A covered entity is required to comply with the administrative requirements of §164.530(b), (d), (e), (g), (h), (i), and (j) with respect to 45 CFR Part 164, Subpart D ("the Breach Notification Rule").		
	Not applicable. Switch is not a covered entity.	
§164.530(b): Training. All workforce members must receive training pertaining to the Breach Notification Rule.		
2.01	Policies and procedures are in place that address training the workforce on the Breach Notification Rules.	No exceptions noted.
2.02	Employees complete training on an annual basis to understand their obligations and responsibilities to comply with the HITECH Breach Notification Rule.	No exceptions noted.
§164.530(d): Complaints. All covered entities must provide a process for individuals to complain about its compliance with the Breach Notification Rule.		
	Not applicable. Switch is not a covered entity.	

#	Control Activity	Results
§164.530(e): Sanctions. All covered entities must sanction workforce members for failing to comply with the Breach Notification Rule.		
	Not applicable. Switch is not a covered entity.	
§164.530(g): Refraining from Retaliatory Acts. All covered entities must have policies and procedures in place to prohibit retaliatory acts.		
	Not applicable. Switch is not a covered entity.	
§164.530(h): Waiver of Rights. All covered entities must have policies and procedures in place to prohibit it from requiring an individual to waive any rights under the Breach Notification Rule as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.		
	Not applicable. Switch is not a covered entity.	
§164.530(i): Policies and Procedures. All covered entities must have policies and procedures that are consistent with the requirements of the Breach Notification Rule.		
	Not applicable. Switch is not a covered entity.	
§164.530(j): Documentation. All covered entities must have policies and procedures in place for maintaining documentation.		
	Not applicable. Switch is not a covered entity.	
§164.402: Definitions: Breach - Risk Assessment. Breach means the acquisition, access, use, or disclosure of PHI in a manner not permitted under subpart E of this part which compromises the security or privacy of the PHI. (2) Except as provided in paragraph (1) of this definition, an acquisition, access, use, or disclosure of PHI in a manner not permitted under subpart E is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors: (i) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification; (ii) The unauthorized person who used the PHI or to whom the disclosure was made; (iii) Whether the PHI was actually acquired or viewed; and (iv) The extent to which the risk to the PHI has been mitigated.		
2.03	Documented escalation policies and procedures are in place to guide employees in reporting, acting upon, and resolving reported events.	No exceptions noted.
2.04	A risk assessment is performed to determine whether a notification must be provided when an impermissible acquisition, access, use, or disclosure of PHI occurs, in accordance with policies and procedures.	No exceptions noted.
2.05	Security personnel monitor access to the facilities' entrances and manage visitor access 24 hours per day to respond to customer inquiries, support issues, and incidents.	No exceptions noted.
2.06	IT personnel utilize an automated ticketing system to document security violations, responses, and resolution.	No exceptions noted.

#	Control Activity	Results
§164.402: Definitions: Breach Exceptions - Unsecured PHI. Breach means the acquisition, access, use, or disclosure of PHI in a manner not permitted under subpart E of this part which compromises the security or privacy of the PHI. (1) Breach excludes: (i) Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part.(ii) Any inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part. (iii) A disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information. (2) Except as provided in paragraph (1) of this definition, an acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:(i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;(ii) The unauthorized person who used the protected health information or to whom the disclosure was made;(iii) Whether the protected health information was actually acquired or viewed; and(iv) The extent to which the risk to the protected health information has been mitigated. Unsecured protected health information means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111-5.		
2.07	Documented escalation policies and procedures are in place to guide employees in reporting, acting upon, and resolving reported events.	No exceptions noted.
2.08	A risk assessment is performed to determine whether a notification must be provided when an impermissible acquisition, access, use, or disclosure of PHI occurs, in accordance with policies and procedures.	No exceptions noted.
2.09	Security personnel monitor access to the facilities' entrances and manage visitor access 24 hours per day to respond to customer inquiries, support issues, and incidents.	No exceptions noted.
2.10	IT personnel utilize an automated ticketing system to document security violations, responses, and resolution.	No exceptions noted.
§164.404(a)(1): Notice to Individuals. A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach. (2) Breaches treated as discovered. For purposes of paragraph (a)(1) of this section, §164.406(a), and 164.408(a), a breach shall be treated as discovered by a covered entity as of the first day on which such breach is known to the covered entity, or, by exercising reasonable diligence would have been known to the covered entity. A covered entity shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity (determined in accordance with the federal common law of agency).		
	Not applicable. Switch is not a covered entity.	
§164.404(b): Timeliness of Notifications. Except as provided in §164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.		
	Not applicable. Switch is not a covered entity.	
§164.404(c)(1): Content of Notification. The notification required by paragraph (a) of this section shall include, to the extent possible:(A) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;(B) A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);(C) Any steps the individual should take to protect themselves from potential harm resulting from the breach;(D) A brief description of what the covered entity is doing to investigation the breach, to mitigate harm to individuals, and to protect against further breaches; and (E) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.(2) The notification required by paragraph (a) of this section shall be written in plain language.		
	Not applicable. Switch is not a covered entity.	

#	Control Activity	Results
§164.404(d): Methods of Notification. The notification required by paragraph (a) of this section shall be provided in the following form:(1) (i) Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as information becomes available. (ii) If the covered entity knows the individual is deceased and has the address of the next of kin or personal representative of the individual (as specified under §164.502(g)(4) of subpart E), written notification by first-class mail to either the next of kin or personal representative of the individual is required. The notification may be provided in one or more mailings as information is available. (2) Substitute notice. In the case in which there is insufficient or out-of-date contact information that precludes written notification to the individual under this paragraph (d)(1)(i) of this section, a substitute form of notice reasonably calculated to reach the individual shall be provided. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of the individual under paragraph (d)(1)(ii).(i) In the case in which there is insufficient or out-of-date contact information for fewer than 10 individuals, then substitute notice may be provided by an alternative form of written notice, telephone, or other means.(ii) In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then such substitute notice shall: (A) Be in the form of either a conspicuous posting for a period of 90 days on the home page of the Web site of the covered entity involved, or conspicuous notice in a major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and (B) Include a toll-free number that remains active for at least 90 days where an individual can learn whether the individual's unsecured protected health information may be included in the breach.(3) In any case deemed by the covered entity to require urgency because of possible imminent misuse of unsecured protected health information, the covered entity may provide information to individuals by telephone or other means, as appropriate, in addition to notice provided under paragraph (d)(1) of this section.		
	Not applicable. Switch is not a covered entity.	
§164.406(a): Notification to the Media. For a breach of unsecured PHI involving more than 500 residents of a State or jurisdiction, a covered entity shall, following the discovery of the breach as provided in §164.404(a)(2), notify prominent media outlets serving the State or jurisdiction.(b)Except as provided in §164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.(c) The content of the notification required by paragraph (a) of this section shall meet the requirements of §164.404(c).		
	Not applicable. Switch is not a covered entity.	
§164.408: Notification to the Secretary. (a) A covered entity shall, following the discovery of a breach of unsecured protected health information as provided in §164.404(a)(2), notify the Secretary.(b) For breaches of unsecured protected health information involving 500 or more individuals, a covered entity shall, except as provided in §164.412, provide the notification required by paragraph (a) of this section contemporaneously with the notice required by §164.404(a) and in the manner specified on the HHS Web site.(c) For breaches of unsecured protected health information involving less than 500 individuals, a covered entity shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification required by paragraph (a) of this section for breaches discovered during the preceding calendar year, in the manner specified on the HHS Web site.		
	Not applicable. Switch is not a covered entity.	
§164.410: Notification by a Business Associate. (a) Standard. (1) General Rule. A business associate shall, following the discovery of a breach of unsecured protected health information, notify the covered entity of such breach. (2) For purposes of paragraph (a)(1) of this section, a breach shall be treated as discovered by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate. A business associate shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the business associate (determined in accordance with the federal common law of agency).(b) Except as provided in §164.412, a business associate shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.(c)(1) The notification required by paragraph (a) of this section shall include, to the extent possible, the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been, accessed, acquired, used, or disclosed during the breach. (2) A business associate shall provide the covered entity with any other available information that the covered entity is required to include in notification to the individual under §164.404(c) at the time of the notification required by paragraph (a) of this section or promptly thereafter as information becomes available.		
2.11	Documented policies and procedures are in place to guide personnel in the procedures for notifying covered entities of a suspected breach within 60 calendar days of discovery.	No exceptions noted.
2.12	IT personnel utilize an automated ticketing system to document security violations, responses, and resolution.	No exceptions noted.

#	Control Activity	Results
2.13	Operations personnel configure priority ratings for tickets created by the ticketing system depending on urgency and impact levels.	No exceptions noted.
2.14	Documented customer support procedures are in place to guide personnel in customer support activities that include, but are not limited to, the following: • **Ticketing** • **Communication to customers** • **Customer complaint resolution** • **Maintenance** • **Event response**	**No exceptions noted.**
§164.412: Law Enforcement Delay. If a law enforcement official states to a covered entity or business associate that a notification, notice, or posting required under this subpart would impede a criminal investigation or cause damage to national security, a covered entity or business associate shall: (a) If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or (b) If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described in paragraph (a) of this section is submitted during that time.		
2.15	Policies and procedures are in place to guide workforce personnel on how to respond to a law enforcement statement that a notice or posting would impede a criminal investigation or damage national security.	No exceptions noted.
2.16	Management complies with law enforcement delay requests for breach notifications.	No exceptions noted.
§164.414(b): Burden of proof. In the event of a use or disclosure in violation of subpart E, the covered entity or business associate, as applicable, shall have the burden of demonstrating that all notifications were made as required by the subpart or that the use or disclosure did not constitute a breach as defined at §164.402.		
2.17	Documented policies and procedures are in place to help ensure that notifications are made as required or that an impermissible use or disclosure did not constitute a breach.	No exceptions noted.
2.18	A risk assessment is performed to determine whether a notification must be provided when an incident results in impermissible acquisition, access, use, or disclosure.	No exceptions noted.
2.19	IT personnel utilize an automated ticketing system to document security violations, responses, and resolution.	No exceptions noted.

SECTION 5

OTHER INFORMATION PROVIDED BY MANAGEMENT

HIPAA PRIVACY REQUIREMENTS

As part of the assessment, Switch reviewed the various privacy safeguards with HIPAA and found them to be not applicable to Switch due to the fact that Switch is neither considered a covered entity nor has any logical access to data. Switch assumes all customers contracting with Switch maintain relationships, either directly or indirectly, with the patient or the payer directly. The requirements under the HIPAA Privacy Rules are primarily the responsibility of the customer.

Schellman noted in the previous section that based on the nature of its services, Switch maintains no logical access to customer data "where the provision of the service involves the disclosure of protected health information from such covered entity" as is referenced in definition of a Business Associate per 45 CFR 160.103. Switch's responsibility is limited to the HIPAA physical and applicable administrative safeguards. Additionally, no technical safeguards from HIPAA or HITECH were tested due to Switch not having access to customer systems.

Limitation

As noted in the opinion letter, a report issued in accordance with SSAE 18, Attestation Standards: Clarification and Recodification, does not provide a legal determination of an entity's compliance with any specified requirements, and as such, the deliverables will not provide a legal determination of Client's compliance with the Specified Requirement.

Use and Disclosures – §164.502

As Switch is not a covered entity, it is not required to follow the use and disclosures requirements set forth in §164.502 – §164.514.

Notice of Privacy Practices §164.520 – §164.530

As Switch is not a covered entity and does not maintain relationships with the patient or payer directly, the notice of privacy practices cited in §164.520 – §164.530 are not applicable.

SOC 1 REPORT

FOR

SWITCH COLOCATION SERVICES

A TYPE 2 INDEPENDENT SERVICE AUDITOR'S REPORT ON A DESCRIPTION OF A SERVICE ORGANIZATION'S SYSTEM AND THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF CONTROLS

FOR THE PERIOD OCTOBER 1, 2022, TO SEPTEMBER 30, 2023

Attestation and Compliance Services

This report is intended solely for use by the management of Switch, Ltd., its user entities (i.e., customers) that utilized the services covered by this report during the specified time period, and the independent financial statement auditors of those user entities (each referred to herein as a "specified user").

If the 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 I

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To Switch, Ltd.:

Scope

We have examined Switch, Ltd.'s ("Switch" or "service organization") description of its Switch Colocation Services system throughout the period October 1, 2022, to September 30, 2023 (the "description"), and the suitability of the design and operating effectiveness of controls included in the description to achieve the related control objectives stated in the description, based on criteria identified in "Management's Assertion" in Section 2 (the "assertion"). The controls and control objectives included in the description are those that management of Switch believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the Switch Colocation Services system that are not likely to be relevant to user entities' internal control over financial reporting.

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

The information included in Section 5, "Other Information Provided by Switch" is presented by management of Switch to provide additional information and is not a part of Switch's description of its Switch Colocation Services system made available to user entities during the period October 1, 2022, to September 30, 2023. Information in Section 5 has not been subjected to the procedures applied in the examination of description of the Switch Colocation Services system and of the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description of the Switch Colocation Services system.

Service Organization's Responsibilities

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

Service Auditor's Responsibilities

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

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA) and International Standard on Assurance Engagements (ISAE) 3402, Assurance Reports on Controls at a Service Organization, issued by the International Auditing and Assurance Standards Board (IAASB). Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, the description is fairly presented, and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period October 1, 2022, to September 30, 2023. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

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

Service Auditor's Independence and Quality Control

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements in the United States of America related to the examination engagement. We have complied with those requirements.

We have also applied the Statements on Quality Control Standards established by the AICPA and the International Standards on Quality Management issued by the IAASB and, accordingly, maintain a comprehensive system of quality control.

Inherent Limitations

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

Description of Tests of Controls

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

Opinion

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

a. the description fairly presents the Switch Colocation Services system that was designed and implemented throughout the period October 1, 2022, to September 30, 2023;

b. the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period October 1, 2022, to September 30, 2023, and as applicable, subservice organizations and user entities applied the complementary controls assumed in the design of Switch's controls throughout the period October 1, 2022, to September 30, 2023; and

c. the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period October 1, 2022, to September 30, 2023, if, as applicable, complementary subservice organization and user entity controls assumed in the design of Switch's controls operated effectively throughout the period October 1, 2022, to September 30, 2023.

Restricted Use

This report, including the description of the tests of controls and results thereof in the Testing Matrices, is intended solely for the information and use of management of Switch, user entities of Switch's Colocation Services system during some or all of the period October 1, 2022, to September 30, 2023, and their auditors who audit and report

on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatement of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than the specified parties.

Scheuman & Company, LLC

Tampa, Florida
November 8, 2023

SECTION 2

MANAGEMENT'S ASSERTION

MANAGEMENT'S ASSERTION

We have prepared the description of Switch, Ltd.'s ("Switch") Colocation Services system throughout the period October 1, 2022, to September 30, 2023 (the "description"), for user entities of the system during some or all of the period October 1, 2022, to September 30, 2023, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risks of material misstatement of user entities' financial statements.

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

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

a. the description fairly presents the Switch Colocation Services system made available to user entities of the system during some or all of the period October 1, 2022, to September 30, 2023, for providing the Switch Colocation Services as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description:

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

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

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

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

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

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

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

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

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

   ii. includes relevant details of changes to the Switch Colocation Services system during the period covered by the description; and

   iii. does not omit or distort information relevant to the scope of the Switch Colocation Services system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and their user auditors, and may not, therefore, include every aspect

of the Switch Colocation Services system that each individual user entity of the system and its auditor may consider important in its own particular environment; and

b. the controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period October 1, 2022, to September 30, 2023, to achieve those control objectives if, as applicable, user entities applied complementary controls assumed in the design of Switch's controls throughout the period October 1, 2022, to September 30, 2023. The criteria we used in making this assertion were that:

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

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

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

SECTION 3

DESCRIPTION OF THE SYSTEM

OVERVIEW OF OPERATIONS

Company Background

Switch is a technology infrastructure ecosystem corporation whose core business is the design, construction, and operation of data centers. Founded in 2000 and headquartered in Las Vegas, Nevada, Switch is built on the intelligent and sustainable growth of the Internet. The Founder and CEO, Rob Roy, has developed more than 700 issued and pending patent claims covering data center designs that manifested into Switch data centers and technology solution ecosystems. Since the opening of their first colocation facility, Switch has delivered 100% uptime across their facilities. At Switch, every team member is driven to produce real results for their clients – technologically and financially. Switch data center ecosystems empower their clients with numerous options for innovation, economies of scale, risk mitigation, sustainability, and investment protection.

Company Profile

Switch's advanced data centers are the center of their platform and provide power densities that exceed industry averages with efficient cooling, while being powered by 100% renewable energy. Two of the Switch data centers are the only carrier-neutral colocation facilities in the world to be certified Tier IV Design, Tier IV Facility, and Tier IV Gold in Operational Excellence. While these certifications have been the highest classifications available in the industry, Switch is building their current facilities to their proprietary Tier 5 Platinum standards, which exceed Tier IV standards. Switch's platform has powerful network effects and nurtures a technology ecosystem that benefits its participants. Switch continues to further enhance these benefits as they innovate and expand their platform ecosystem. Switch currently has over 1,000 customers, including technology and digital media companies, cloud, and managed service providers, financial institutions, and telecommunications providers.

The growing nexus between Internet connectivity, Internet-based services, data and analytics, and the advancement of computational processing power is rapidly expanding the amount of data that enterprises can access and manage. At the same time, the Internet of Everything is exponentially expanding the available data sources, as utility grids, automobiles, aircraft, home appliances, wearable devices, and numerous other sources are all connecting to the Internet. The compute capacity necessary to manage and analyze this data is also advancing and demanding increasing amounts of power to operate. Switch believes that traditional technology infrastructure is not capable of supporting the growing wave of mission critical data and increasingly powerful IT equipment.

Switch presently owns and operates four primary campus locations, called Primes, which encompass fourteen colocation facilities with an aggregate of over 5.3 million gross square feet (GSF) of space. These facilities have approximately 470 megawatts (MW) of power available to them. Primes consist of The Core Campus in Las Vegas, Nevada; The Citadel Campus near Reno, Nevada; The Pyramid Campus in Grand Rapids, Michigan; and The Keep Campus in Atlanta, Georgia. Primes are strategically located in geographies that combine a low risk of natural disaster, favorable tax policies for customers deploying computing infrastructure, and low latency connectivity to major metropolitan markets, such as Los Angeles, San Francisco, Silicon Valley, Chicago, New York, Northern Virginia, and Miami. As a result, customers in these metropolitan markets can access Switch's colocation facilities while reducing exposure to higher taxes, higher cost of power, and higher risk of natural disaster that might be prevalent in other markets. Switch can also use their Switch Modular Optimized Design (MOD) technology to build single-user facilities and are actively pursuing opportunities to deploy this technology in a build-to-suit offering for their enterprise customers.

As additional locations and sectors within the four existing Prime campus locations are opened for Colocation Services, the same / similar controls tested within this report are implemented / in place.

Description of Services Provided

Physical Security

Exterior Barriers

From well-defined perimeters consisting of signage, blast walls, and gates, to clear avenues of approach and backup perimeter barriers, the first layer of physical security is extensive. Exterior walls are constructed of either steel reinforced poured concrete or masonry reinforced beyond building code requirements. Entry points are kept to a minimum and each exterior door is reinforced, alarmed, access-controlled, and viewed by two dedicated fixed cameras.

Interior Barriers and Customer Compartmentalization

Exterior doors lead into specially engineered mantraps built over fire corridor wall construction. The mantraps are sheeted with steel and seams are strapped by aluminum. Access points off the mantrap require additional multi-factor biometric authentication of the card holder and are controlled via a 24 hour per day security officer and mantrap relay logic. Each mantrap includes fixed cameras viewing each door.

Each customer space, whether it is a cage, cabinet, or suite, is individually locked, protected, and monitored. Additional security safeguards, such as mantraps, intrusion sensors, and surveillance cameras, can be added to these spaces at the customer's request.

Positive Access Control

Positive Access Control is the application of a two-fold access principle stemming from the questions, "Who are you? And why should we let you in?" When first granted access to the facility, a multi-step process is in place to determine identity and verify need for access. In addition to the metal walls, turnstiles, cameras, intercoms, and biometric readers, Switch's access control takes on further hardening by the Positive Access Control procedures deployed at the facilities. Positive Access Control requires that a proprietary 24 hours per day officer staffed security command center (SECOM) verifies that the person standing in the mantrap matches a file photo. After confirmation, the officer activates the second proximity and biometric reader for use.

The access process is further continued with periodic access audits performed each shift by the shift supervisor. Customer audits are conducted monthly by the campus security manager. A complete audit of personnel with access to the facilities is conducted by the Security Director on a semi-annual basis.

Surveillance

Surveillance equipment for the facilities follows an elite standard set by a board-certified security professional. Fixed cameras are high-resolution color (520 lines) or digital high definition (HD) with automatic low light switching, capable of viewing up to 0.1 lux. Pan / tilt / zoom (PTZ) cameras are used on the exterior and areas of sensitivity. Video is digitally recorded at common interchange format (CIF) resolution at 15 images per second (IPS) upon motion at 4CIF 30 IPS upon operator command or at select zones requiring enhanced video. Video is retained for 100 +/- 10 days.

Switch deploys active surveillance with on-staff officers operating the camera system 24 hours per day. Camera operators use the Identify, Observe and Understand (IOU) methodology. The IOU methodology includes constant monitoring, use of cameras for detection, and a usable video product for investigations.

Sensors

Detectors are used around the property and provide early warning for perimeter and sensitive area intrusion. Sensor types include infrared motion, ultrasonic motion, photoelectric motion, electromechanical, internal lock, and seismic. These sensors are installed based on the environment or protection needs.

Security Team

Switch has a proprietary SECOM fully staffed 24 hours per day. Security staff members are hired with military and law enforcement security experience and must complete an extensive training period, which includes security system instruction, procedure and policy instruction, and non-lethal weapon training. The Security Academy was developed in accordance with the current American Society for Industrial Security (ASIS) International Guideline on

Private Security Officer Selection and Training (ASIS GDL PSO-2010) and the 90-day field training officer (FTO) program. A security supervisor oversees each shift and reports to the campus security manager. Security supervisors are required to attend a Security Management course, and officers in management positions are required to be active members of ASIS International.

Please refer to the following link for related pictures and detailed information: http://www.switch.com.

Infrastructure Operations (Environmental Security)

Switch employs the latest advanced environmental controls to protect the systems of its customers as well as operating with energy efficiency. These systems are managed and monitored by the Data Center Operations (DCO) and Energy Management Systems (EMS) teams.

Fire Protection

Fire protection includes fire, smoke, and heat detection monitored 24 hours per day. Sensors are located throughout the data centers and provide alerts to physical security personnel and a third-party monitoring company for response. Data center areas are protected by aspirating smoke detectors, which are programmed to identify smoke in the incipit stage.

The data centers are equipped with dual-interlock pre-action dry pipe sprinklers. Specifically, these dual-interlock pre-action sprinklers require both a smoke detection event and the activation of sprinklers to release water into the pipes. This allows for quick response to a fire with a lower risk of water damage in the case of a smaller fire or false alarm.

Heating, Ventilation, and Cooling (HVAC)

Switch utilizes advanced, patented techniques starting with a custom-designed thermal separate compartment in facility or (t-scif) air-flow system. This airflow system pulls the warm air away from customer systems into a separate compartment. The warm air is taken out of the core SUPERNAP facility designed for 74 high-grade Switch-designed and patented TSC-600 and TSC-1000 HVAC units which are physically adjacent to the data center, each containing six types of air conditioning systems. Within the data centers, areas where warm or hot air travels are marked in red.

Please refer to the following link for related pictures and detailed information: http://www.switch.com.

Power Management

Switch utilizes multiple in-bound connections from electricity providers. Tri-redundant power systems, which balance dual in-bound power connections across three sources of power, optimize the power utilization. Power is currently provided in redundancy through the use of uninterruptable power supply (UPS) devices which are fed by generators across the campuses. Power distribution units are managed and secured to prevent tampering. Power cabling within the data center is color-coded for quick and succinct identification of circuits and to assist with troubleshooting.

Please refer to the following link for related pictures and detailed information: http://www.switch.com.

Support for Colocation Services

Switch maintains dedicated support for its customers 24 hours per day via the Network Operations Center (NOC). NOC and engineering staff are available to assist with network troubleshooting and provide "hands-on" services to support customers.

NOC representatives follow defined procedures to facilitate confirmation of identification, customer communication of unexpected events that may impact their systems, customer authorization (only authorized customer representatives can open a service request), and functional escalation for customer service requests and incidents. NOC representatives monitor customer inquiries, support issues, and incidents on a real-time basis. Issues are documented in the Living Data Center (LDC) ticketing system and tracked to resolution.

The ticketing system / customer relationship management (CRM) system contains a complete purchased product hierarchy, installed equipment, and the physical and logical infrastructure layouts of individual customer solutions.

The complete history of customer service requests and incidents are recorded in the ticketing system. Customer-specific information is handled confidentially through permission-access levels in the ticketing system and access to customer infrastructures. Documented procedures are in place for the monitoring of customer support operations. Furthermore, volume analysis, response times, and procedural adherence are monitored to help ensure customer obligations are met.

Network Management and Monitoring (Logical Security)

Since Switch has no logical access to any customer's equipment or data, each customer is responsible for its own network security. Switch manages the network connectivity to the Internet via its multiple providers. Switch's core routers are managed by the network engineering team and monitored by the NOC 24 hours per day. Routers are configured for high availability in active-active mode such that if one fails or connectivity is lost, network traffic is diverted accordingly.

Switch's Colocation Services system environment is an information technology general control (ITGC) system, and user entities are responsible for the procedures, by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to reports and other information presented to them; additionally, user entities are responsible for the procedures and controls governing the related accounting records, supporting information, and specific accounts that are used to initiate, authorize, record, process, and report transactions processed within Switch's Colocation Services system; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for those user entities.

System Boundaries

The scope of this report is limited to the Colocation Services for the following facilities:

- Las Vegas, Nevada
  - Las Vegas 2 (LAS 2)
  - Las Vegas 4 (LAS 4)
  - Las Vegas 5 (LAS 5)
  - Las Vegas 7 (LAS 7)
  - Las Vegas 8 (LAS 8)
  - Las Vegas 9 (LAS 9)
  - Las Vegas 10 (LAS 10)
  - Las Vegas 11 (LAS 11)
  - Las Vegas 12 (LAS 12)
  - Las Vegas 15 (LAS 15)
- Reno, Nevada
  - Reno 1 (RNO 1)
  - Reno 2 (RNO 2)
- Grand Rapids, Michigan
  - Grand Rapids 1 (GRR 1)
- Atlanta, Georgia.
  - Atlanta 1 (ATL 1)

The Colocation Services include the physical infrastructure, power, and data connectivity needed to house information systems of user entities. Switch provides certain physical and environmental security mechanisms to safeguard user entities' physical assets from unauthorized access and environmental threats. The specific control objectives and related control activities included within the scope of this engagement can be found in Section 4 of this report.

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 system components described below.

Infrastructure and Software

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

Primary Infrastructure			
Production System	**Business Function Description**	**Operating System Platform**	**Physical Location**
The Living Data Center (LDC) Application	Overall environmental conditions monitoring as well as ticketing system capability to track incidents and resolutions.	Linux	Las Vegas, Nevada Reno, Nevada Grand Rapids, Michigan Atlanta, Georgia
Microsoft Active Directory Domain	Network domain supporting internal systems applicable to the Colocation Services.	Windows	
Cisco Border and Private Routers	Network devices in place to direct traffic and filter unauthorized inbound network traffic from the Internet.	Cisco Internetwork Operating System (IOS)	
Honeywell Badge Access System	Physical access control supporting the Colocation Services at the Las Vegas, Reno, and Grand Rapids facilities that was decommissioned during November 2022. The in-scope facilities using Honeywell transitioned to C-Cure prior to the end of November 2022.	Windows	
C-Cure Badge Access System	Physical access control supporting the Colocation Services at the Las Vegas, Reno, Grand Rapids, and Atlanta facilities.		

In addition, Switch utilizes CrowdStrike antivirus software for antivirus protection for the Windows production servers and workstations. Furthermore, Switch utilizes Milestone Video Management System (VMS) for managing the security cameras for the interior and exterior of the data centers.

Functional Areas of Operations

Switch utilizes specific functional areas of operations that support the scope of this review that include, but are not limited to, the following:

- Executive Management – responsible for overseeing company-wide activities, establishing, and accomplishing goals, and overseeing objectives.
- Security Operations (SecOps) department – responsible for monitoring and protecting the facility from unauthorized access, damage, and interference.
- Network Operations (NetOps) department – responsible for implementation of product development and optimization, client implementation, and technical operations.
- Data Center Operations (DCO) – responsible for monitoring and maintaining critical infrastructure including electrical and cooling infrastructure. Also responsible for preparing customer environment (cage, cabinet) and performing everyday maintenance of the facility.
- Energy Management Systems (EMS) department – responsible for monitoring and maintaining critical infrastructure including power equipment and infrastructure.
- Network Engineering department – responsible for managing network architecture.
- Facilities Services department – responsible for providing user entities with assistance before and after the initial sale by providing information, guidance, and continued support.
- Human Resources (HR) department – responsible for HR policies, practices, and processes with a focus on key HR department delivery areas (e.g., talent acquisitions, employee retention, compensation,

employee benefits, performance management, employee relations, development, and employee-related incidents and investigations).

- **Legal department – responsible for legal and regulatory issues involving corporate risk and corporate compliance.**

Data Management

Badge access logs and video surveillance recordings are a key component of the Colocation Services provided by Switch. The logs and recordings are reviewed on a real-time basis by SECOM and retained for forensic purposes. Customer data was not included in the scope of this examination as Switch is not responsible for the administration or maintenance of customer systems or data.

Subservice Organizations

No subservice organizations were applicable to the scope of this examination.

Switch's Colocation Services system was designed with the assumption that no subservice organization controls were required in the design of Switch's controls; therefore, no control objectives related to Switch's Colocation Services system are dependent upon complementary subservice organization controls that are suitably designed and operating effectively, along with the related controls at Switch.

Significant Changes During the Period

The Reno 02 (RNO 02) data center facility was operational as of May 1, 2023. The test of controls at the facility only apply to the facility's dates of operation during the specified reporting period of May 1, 2023, to September 30, 2023, for the Reno 02 data center facility.

CONTROL ENVIRONMENT

The control environment at Switch is the foundation for the other areas of internal control. It sets the tone of the organization and influences the control consciousness of its personnel. The components of the control environment factors include the integrity and ethical values, management's commitment to competence, its organizational structure, the assignment of authority and responsibility, and the oversight and direction provided by the Board of Managers 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 Switch's control environment, affecting the design, administration, and monitoring of other components.

Integrity and ethical behavior are the product of Switch's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct. Specific control activities that Switch has implemented in this area are described below:

- An employee manual is utilized to document organizational policy statements and codes of conduct and communicate entity values and behavioral standards to personnel.
- Policies and procedures require that employees sign an acknowledgment form indicating that they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
- Employees must sign a confidentiality statement agreeing not to disclose proprietary or confidential information, including customer information, to unauthorized parties.

- Background screenings are performed for employee candidates as a component of the hiring process.
- Drug screening tests are performed for employee candidates as a component of the hiring process.
- As security is core to Switch's services, employees and contractors are required to attend security orientation and awareness training as a component of the hiring process and on an ongoing basis.

Board of Managers and Audit Committee Oversight

Switch's control consciousness is influenced significantly by its Owners and Board of Managers' participation. A Board of Managers is in place to oversee management activities and meets on a periodic basis.

Organizational Structure and Assignment of Authority and Responsibility

Switch's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Switch's management believes that establishing a relevant organizational structure includes considering key areas of authority and responsibility and lines of reporting. Switch has developed an organizational structure suited to its needs. This organizational structure is based, in part, on its size and the nature of its activities.

Switch's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to business practices, knowledge and experience of key personnel, and resources provided for carrying out duties.

In addition, it includes policies and communications directed at ensuring that personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable. Organizational charts are in place to communicate key areas of authority, responsibility, and lines of reporting to personnel. The charts are communicated to employees and updated as needed.

Commitment to Competence

Switch management defines competence as the knowledge and skills necessary to accomplish tasks that define an employee's roles and responsibilities. Switch'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.

Management ensures employees have adequate training to carry out their job responsibilities. This includes Switch's self-developed Security Academy where security personnel undergo incremental training in facilities security as well as Switch's physical security processes and supporting technology.

Accountability

Switch's management philosophy and operating style 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. Specific control activities that Switch has implemented in this area are described below:

- Input and feedback are actively sought from and provided by Switch customers and partners.
- Management is periodically briefed on regulatory and industry changes affecting the services provided.
- Management meetings are held on a periodic basis to discuss operational issues.

Switch's HR policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities. Specific control activities that Switch has implemented in this area are described below:

- **Management has established pre-hire screening procedures which are performed for employee candidates.**
- **New hire onboarding includes, but is not limited to, the following elements:**
  - **Verification that the employee has signed the employee agreement;**
  - **Verification that the employee has signed the confidentiality agreement;**
  - **Verification that the employee has signed an acknowledgment of receipt of employee handbook document; and**
  - **Verification that the employee has taken security training and signed an acknowledgment of such training.**
- **Management utilizes termination procedures which include, but are not limited to, the following elements:**
  - **Collection of company property;**
  - **Revocation of physical and system access rights; and**
  - **Signatures of each person that performs requisite tasks.**
- **Evaluations are performed for employees on an annual basis.**

RISK ASSESSMENT

Security and risk management are of primary importance to Switch. Switch's management has placed into operation a risk assessment process to identify and manage risks that could affect the organization's ability to provide reliable Colocation Services for user entities. Management is responsible for identifying the risks that threaten the achievement of the control objectives stated in management's description of the services. Management has implemented a process for identifying relevant risks. This process includes estimating the significance of identified risks, assessing the likelihood of their occurrence, and implementing measures to address those risks.

Objective Setting

Switch faces a variety of risks from external and internal sources, and a precondition to Switch's risk assessment methodology is the establishment of objectives, linked at different levels and internally consistent. Objectives are set at the strategic level, establishing a basis for operations, reporting, and compliance objectives. Objectives are aligned with Switch's risk appetite, which drives risk tolerance levels.

More specific objectives flow from the entity's broad strategy. Entity-level objectives are linked and integrated with more specific objectives established for various "activities," such as sales, marketing, and operations, making sure they are consistent. These sub-objectives, or activity-level objectives, include establishing goals and may deal with product line, market, financing, and profit objectives.

By setting objectives at the entity and activity levels, Switch can identify success factors. Success factors exist for the entity, a business unit, a function, a department, or an individual. Objective setting enables management to identify measurement criteria for performance, with focus on success factors. Switch has established certain broad categories including:

- Operations objectives – these pertain to effectiveness and efficiency of the operations, including performance and delivery goals and safeguarding resources against loss. They vary based on management's choices about structure and performance.

- Compliance objectives – these objectives pertain to adherence to laws and regulations to which Switch and their customers are subject. They are dependent on external factors, such as government and industry regulation.

Risk Identification

Regardless of whether an objective is stated or implied, Switch's risk-assessment process considers risks that may occur. Switch has considered significant interactions between itself and relevant external parties and risks that could affect the organization's ability to provide reliable service to its user entities.

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, incentives, pressures, opportunities, attitudes, and rationalizations
- A disruption in information systems processing
- The quality of personnel hired, and methods of training utilized
- Changes in management responsibilities
- The nature of the entity's activities and employee accessibility to assets

The Switch risk assessment process focuses on supporting management decisions and responding to potential threats by assessing risks and identifying important decision factors. Executive management oversees risk management ownership and accountability. Senior management from different operational areas is involved in the risk identification process. Management identifies elements of business risk including threats, vulnerabilities, safeguards, and the likelihood of a threat, to determine the actions to be taken.

Potential for Fraud

The potential for fraud is considered 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 misappropriation 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. Documented policies and procedures are in place to guide personnel in identifying the potential for fraud as part of the risk assessment process. Additionally, the annual risk assessment considers the potential for fraud.

Risk Analysis

Switch's methodology for analyzing risks varies largely because many risks are difficult to quantify. Nonetheless, the process usually includes:

- Estimating the significance of a risk;
- Assessing the likelihood (or frequency) of the risk occurring; and
- Considering how the risk should be managed (i.e., an assessment of what actions need to be taken).

Risk analysis includes identification of key business processes where potential exposures of some consequence exist. Once the significance and likelihood of risk have been assessed, management considers how the risk should be managed. This involves judgment based on assumptions about the risk and reasonable analysis of costs associated with reducing the level of risk.

Necessary actions are taken to reduce the significance or likelihood of the risk occurring.

Risk Mitigation

Risk mitigation activities include the ability to identify, select, and develop activities that sufficiently meet the identified risks. However, the relative costs versus benefits should also be considered when determining the risk mitigation activities. The organization has documented policies and procedures to guide personnel throughout this process. The annual risk assessment and mitigation process also addresses risks arising from potential business disruptions.

Vendors and business partners are also considered during the annual risk assessment and mitigation process. Documented policies and procedures are in place to guide personnel in identifying risks associated with vendors and business partners as part of the risk assessment process. Monitoring procedures are also in place to ensure continual compliance by vendors and business partners. This includes reviewing vendor audit reports and/or security questionnaires at least annually.

Integration with Control Objectives

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

CONTROL OBJECTIVES AND RELATED CONTROL ACTIVITIES

Selection and Development of Control Activities

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

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

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

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

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

Organization and Administration

Control Objective: Control activities provide reasonable assurance that discipline and structure are an integral part of the organization and influence the control consciousness of its personnel.

A Board of Managers is in place to exercise control and management over the organization, which includes overseeing management activities. Management has defined, developed, and communicated an organizational chart to communicate areas of authority and responsibilities. In addition, an employee manual is in place to communicate policies and procedures regarding codes of conduct, entity values, and behavioral standards. Employees are required to sign an acknowledgment form upon hire indicating that they have been provided a copy of the handbook, been informed where to access the handbook, have read the handbook, and agree to abide by the policies, procedures, rules, and protocols contained in the handbook. Management also requires employees to complete a training program to help ensure that employees have the necessary training to carry out their responsibility.

HR Management

Control Objective: Control activities provide reasonable assurance that employee onboarding and offboarding procedures are utilized to ensure compliance with company policies and security practices.

Switch has documented policies and procedures for employee onboarding and offboarding. Candidates go through a rigorous interview process during the hiring process. To minimize the risk of malicious behavior, potential employees and contractors who have and will have access to the data center undergo the following verifications:

- Background screenings that include examination of criminal conviction records and social security number (SSN) verification, credit history, driving records, personal information, employment comparison, public records check, and a global homeland security check. The background investigation commences once an offer of employment has been communicated and accepted. Conditional employment offers are made contingent on successful completion of background checks and no access is permitted prior to the background check being completed.
- Drug screening tests that include a standard five-panel plus extra tests for "ecstasy" (MDMA) and OxyContin / Oxycodone. Conditional employment offers are made contingent on successful completion of a clean drug test.

Once an employee has decided to join Switch, they attend a mandatory new hire orientation on their first day of employment that includes a review of the employee handbook, the signing of the confidentiality agreement acknowledgment form, and a security orientation. In addition, management requires a security orientation for customers and vendors who will be granted access to the facilities using a badge.

Switch performs specific actions to remove system access and collect any company property from employees upon their departure. During the termination process, a termination ticket is completed to document that the employee

returned such items as their access badge, company property (e.g., laptop), and that their system accounts and physical access privileges were removed.

Physical Security

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

Switch has implemented various physical security protocols to protect the business premises and information systems from unauthorized access. A badge access system is in place 24 hours per day to control access to the office. Predefined access groups are utilized to provide access depending on the individual's role and responsibilities. Physical access to the data center is documented and approved by the employee's manager prior to access being granted, while physical access to customer cages is documented and approved by the customer prior to access being granted. Badge access attempts are logged by the system and are traceable to specific badge access cards. Management reviews employee and customer access privileges on a semi-annual basis. The ability to administer the badge access system is restricted to authorized security management personnel. If an individual who has physical access to the Switch facilities is terminated, security management personnel revoke the badge access privileges within 24 hours as a component of the termination process.

The building perimeters for the facilities include fences, walls, and entrance gates controlled by guards or card access. In addition, surveillance cameras are utilized by security personnel to monitor the main entrance to the facilities in order to identify visitors and contractors prior to granting access to the facilities. Visitors must present photo identification before being granted access to the facilities. Personnel at the facilities are distinguished as being an employee, customer, or contractor with a functioning color-coded badge access card or a visitor with a non-functioning visitor badge. Prior to being granted access to the secure interior of the data centers, personnel and authorized customers must enter a mantrap where they must scan the badge access card and provide biometric credentials. Personnel and authorized visitors are required to provide badge access cards and biometric identification for both entry and exit of interior doors. Visitors without badge access cards are required to be escorted by authorized employees while within the facilities.

Switch maintains and monitors activity logs of certain physical movements within the facilities on an as needed basis. Physical movements captured and monitored include date / time, event, badge access card details, and device. Digital surveillance cameras are in place to monitor the facility entrances, the building perimeters, and other areas within the facilities. Video surveillance captured by the camera system is archived allowing the capability for review as needed. The facilities are monitored 24 hours per day by security personnel with the use of motion-sensitive digital surveillance cameras, alarms, and motion detectors. The physical security hardware (e.g., monitoring servers, DVRs) is secured behind locked server racks and physical cages. An incident reporting system is utilized by security personnel to document any physical security incidents.

Environmental Security

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

Switch has implemented various environmental security protocols to protect the business premises and information systems from potential environmental issues. The Switch facilities are protected by fire detection and suppression equipment that includes fire alarms, dry-pipe water sprinklers, fire and smoke detectors, hand-held fire extinguishers, and smoke and heat sensors. On a quarterly basis, the fire detection and suppression equipment undergo an inspection from a third-party specialist to help ensure that the equipment is in proper working order. Hand-held fire extinguishers undergo maintenance inspections on an annual basis.

Management utilizes an environmental monitoring tool which is configured to systematically monitor the humidity and temperature levels within the Switch data centers. The system is configured to automatically send e-mail notifications to operations personnel when predefined thresholds are exceeded. An inspection matrix guides the frequency of inspection for critical infrastructure including power and cooling systems.

The data centers are designed to optimize cool air flow and utilize redundant air conditioning units to keep infrastructure equipment at optimal temperatures. On a quarterly basis, the air conditioning systems undergo an inspection from a third-party specialist to help ensure that the equipment is in proper working order. The facilities are equipped with multiple UPS systems and diesel generators to provide electricity in the event of a power outage. The data centers also contain two distinct electrical connections to the electrical company's substation. Utility power is run through the UPS battery systems so that customers receive clean, conditioned battery power. In the event that a loss of utility power occurs, the generators will engage and begin supplying power to the UPS systems. Whether it is from utility or generator power, each customer draws power from the UPS battery systems, ensuring smooth transitions from utility to generator and back again. On a semi-annual basis, UPS inspections are performed, and on a quarterly basis, generator inspections are performed to help ensure that the systems are in proper working order. Additionally, internal personnel perform preventative maintenance procedures on the UPS systems and generators on a quarterly basis.

Logical Security

Control Objective: Control activities provide reasonable assurance that logical access to network infrastructure is restricted to authorized personnel.

Redundant routers are in place at the data center to provide Internet connectivity for customers. Network infrastructure devices restrict user access to Internet communication sessions originating from a predefined list of IP addresses. In order to gain access to the routers, a user must authenticate with a user account and password via a secure shell (SSH) program to help ensure that the sessions are encrypted. The routers may only be managed from an internal network as SSH is not running on the public portion of the routers. SSH sessions are programmed to terminate a session after a predefined period of inactivity.

The network engineering team manages the security administration of the routers and is required to authenticate through a terminal access controller access-control system plus (TACACS+) server which allows for individualized user account access, administration, and logging. These unique user accounts are defined by the TACACS+ server and are configured to authenticate using the corporate network domain. The network domain is configured to enforce password requirements that include minimum length, expiration intervals, complexity, minimum history, and invalid account lockout threshold.

Management has restricted administrative access privileges within the routers to authorized personnel. Furthermore, the TACACS+ server is configured to log successful and unsuccessful login attempts and administrator commands executed during an active session. IT management reviews these logs on an ad hoc basis to determine if any suspicious or unauthorized activity has occurred.

Network Monitoring and Problem Management

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

Switch has implemented an internally developed custom built application called SYSLOG to monitor the performance and availability of customer network infrastructure including switches, routers, servers, and media converters. The routers are in place at the data center to provide network connectivity for customers. Routers are configured for redundancy such that if one fails, network connectivity is still available to customers. The network infrastructure is monitored 24 hours per day by NOC technicians to assist with network issues. Management has implemented procedures to guide NOC technicians in identifying and responding to network related incidents as well as incident response and escalation procedures in the event that an event is detected.

A proprietary ticketing system, LDC, was developed and is utilized to handle network related issues in order to manage, track, and respond to network issues until resolution. When an issue is detected, NOC technicians will examine the issue and create a ticket to assign priority level on a scale (1-5) based on the urgency and impact of the incident to the business and/or the customer, and to determine predefined timelines to resolve the issue.

If the issue cannot be resolved within the predefined timeline, escalation procedures have been implemented to get the necessary personnel involved to resolve the issue. Once the issue is fixed, the NOC technician will update the support ticket with full details of the issue fix.

Customer Support

Control Objective: Control activities provide reasonable assurance that dedicated customer support personnel are in place to handle customer communications and that issues are escalated according to predefined procedures.

Switch has implemented standard procedures, including escalation procedures, to provide timely and consistent communication to customers. These procedures apply to Switch employees and contractors responsible for providing customer support. In addition, NOC personnel are available 24 hours per day to respond to customer inquiries.

Customers communicate incidents by phone, e-mail, or the LDC customer portal. NOC personnel verify that the request was initiated by an authorized customer contact. In the event that the request was initiated by an unauthorized customer contact, NOC personnel place the request on hold until the authorization is granted, or the request is confirmed by the authorized contact.

Once the customer contact is confirmed, the NOC technician opens a ticket within LDC and attempts to troubleshoot the issue. If the ticket is not responded to within a predefined timeline based on its severity, the ticketing system is configured to notify Switch personnel of the open ticket until the ticket is addressed. If the issue cannot be resolved, the assigned NOC technician will notify the responsible department and/or vendor through a predetermined set of contacts. Once the affected departments have been notified of the issue, e-mail updates are sent out on an as needed basis until the issue is resolved and ticket is closed.

Customer Provisioning

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

A formal, documented customer provisioning set of standards and procedures are in place to guide personnel in provisioning new customers and to help ensure that each customer receives the service(s) requested. The sales teams consult with the customer to build an acceptable quote for desired products and services.

Once a solution with corresponding pricing has been developed, Switch requires a signed colocation facility services agreement with the customer prior to beginning customer provisioning activities. The agreement includes the agreed upon services to be performed as well as a provisioning questionnaire that documents key personnel contact information, connectivity requirements, redundancy specifications, and other information related to the installation or change of service.

Upon receiving the signed agreement from the customer, Switch assigns the responsibility to a project manager for ensuring that the customer is provisioned according to the customer's specifications and expectations. The project manager works with various teams within Switch to help ensure the successful implementation of the services requested on the customer order. The project manager, the customer, and internal departments work together to forecast an estimated order completion date, which is monitored through regular status updates. If any changes to the estimated order completion date occur, they are communicated to the customer during status updates or through e-mail communications.

After the customer cage or cabinet has been set up within the data center, engineering diagrams are developed and/or updated to reflect the proposed solution. The diagrams are maintained and available online for the customer's use. The project manager then schedules a new customer welcome call. During this call, members of the IT and operations groups go over the customer cage or cabinet set up process and provide the customer with Switch policies and procedures.

INFORMATION AND COMMUNICATION SYSTEMS

Relevant Information

Carriers and Connectivity

Switch has direct connections to many of the national Internet backbones. Its specific carriers are:

- Atlantic Telenetwork (Comnet)
- 123net
- Arelion
- Astound
- AT&T
- ATT Michigan (Michigan Bell Telephone Company)
- Bandwidth Infrastructure Group (BIG)
- Casair
- CC Communications
- Charter
- Cogent
- Comcast
- Cox
- Crown Castle (formerly Wilcon)
- Everstream (formerly Comlink)
- Global Telecom & Technology (GTT)
- IX Reach
- Lumen
- Masergy
- Megaport
- Packet Fabric
- Parker Fiber
- Pacific Century CyberWorks (PCCW) Limited
- Roberts
- Sky Fiber
- Tata
- Telepacific
- Telia
- Time Warner Cable
- T-Mobile (formerly Sprint)
- US Signal
- Valley Electric (VEA)
- Verizon
- Windstream
- Zayo

Network Design

Data centers are connected diversely and redundantly by Switch-owned fiber. Every data center has multiple pathways to the other data centers to take advantage of a broad blend of multiple providers on two different autonomous systems. This design succeeds in being dynamic, robust, and diverse.

Customers who collocate in one of the Switch facilities are provided a number of different options for Internet connectivity. These range from single drops to multiple redundant drops. Redundancy to the customer is provided either by Border Gateway Protocol (BGP) or Hot Standby Routing Protocol (HSRP).

The network core is built upon a platform of carrier-class equipment which services Switch's user entities. The border routers are meshed together to the core to maximize the ability to transport data to the optimal provider. Conversely, by having multiple providers, a customer's data is received in a fast and efficient method. Customers have the ability to choose between BGP, HSRP, and single connection routing.

Switch extends its availability into Southern California to the prominent One Wilshire Building. This presence enables Switch to peer with more than 50 international telecommunications companies.

Communication

Switch has implemented various methods of communication to help ensure that employees understand their individual roles and responsibilities for Colocation Services and controls, and to help ensure that significant events are communicated. These methods include orientation and training programs for newly hired employees and the use of electronic mail messages to communicate time-sensitive messages and information. Managers also hold periodic staff meetings.

MONITORING

Monitoring Activities

At the executive level, controls are monitored to consider whether they are operating as intended or require modification for changes in conditions. Switch's management performs monitoring activities to continuously assess the quality of internal control over time. Monitoring activities occur on a continuous basis and necessary corrective actions are taken as required to correct deviations from company policy and procedures. This process is accomplished through ongoing monitoring activities and separate evaluations.

The Switch management team conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through management meetings, customer conference calls, and informal notifications.

Management's close involvement in the operations can identify significant variances from expectations regarding internal controls. Upper management immediately evaluates the specific facts and circumstances with any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in Switch's procedures or personnel. The goal of this process is to ensure legal and regulatory compliance, as well as to maximize the performance of Switch personnel.

Switch utilizes the LDC system for overall monitoring. The platform includes an incident ticketing system as well as real-time monitoring capabilities. With respect to the previously mentioned control activities, the following are key monitoring controls:

- Video surveillance for physical security
- Physical access logs
- Semi-annual customer access reviews
- Motion detection sensors
- Fire, smoke, and heat detection sensors
- Temperature and humidity monitors monitored by critical infrastructure staff
- Air flow sensors monitored by critical infrastructure staff
- Network device health monitoring with real-time alerts sent to network operations staff
- Logical access logs identifying authorized, unauthorized, and administrative activities on key network devices and platforms

Additionally, Switch has periodic security assessments in accordance with the Department of Homeland Security (DHS) Argonne model.

Reporting Deficiencies

Deficiencies in an entity's internal control system surface from many sources, including the company's ongoing monitoring procedures, separate evaluations of the internal control system, and external parties. Management has

developed protocols to help ensure that findings of internal control deficiencies are reported not only to the individual responsible for the function or activity involved, who is in the position to take corrective action, but also to at least one level of management above the directly responsible person. This process enables that individual to provide needed support or oversight for taking corrective action, and to communicate with others in the organization whose activities may be affected. Management evaluates the specific facts and circumstances related to deficiencies in internal control procedures and makes the decision for addressing deficiencies based on whether the incident was isolated or requires a change in the company's procedures or personnel.

COMPLEMENTARY CONTROLS AT USER ENTITIES

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

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

Control Activities Expected to be Implemented at User Entities	Related Control Objective
User entities are responsible for implementing monitoring controls to detect and alert the user entity of actual or attempted security breaches to their network(s) and infrastructure.	Logical Security
User entities are responsible for ensuring that firewall and system logging are enabled and sufficient for their purposes.	
User entities are responsible for implementing a security infrastructure and practices to prevent unauthorized access to their internal network and limit threats from connections to external networks.	
User entities are responsible for creating and communicating to Switch specific escalation procedures for problems with their network services.	Network Monitoring and Problem Management
User entities are responsible for notifying Switch of changes to their points of contact.	Customer Support
User entities are responsible for completing the provisioning questionnaire accurately and completely.	Customer Provisioning

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 Switch. The scope of the testing included the applicable controls for the Switch Colocation Services system considered to be relevant to the internal control over financial reporting of respective user entities. Schellman & Company, LLC (Schellman) conducted the examination testing over the period October 1, 2022, through September 30, 2023.

Tests of Operating Effectiveness

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

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

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

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

Sampling

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

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

Test Results

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

ORGANIZATION AND ADMINISTRATION

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that discipline and structure are an integral part of the organization and influence the control consciousness of its personnel.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.01	Organizational charts are in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel. These charts are communicated to employees and updated as needed.	Inquired of the Director of IT Compliance regarding the communication of organizational charts to employees to determine that organizational charts were in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel and that these charts were communicated to employees and updated as needed.	No exceptions noted.
		Inspected the organizational charts to determine that organizational charts were in place and communicated key areas of authority, responsibility, and lines of reporting.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.02	An employee manual is utilized to document organizational policy statements and codes of conduct and to communicate entity values and behavioral standards to personnel.	Inspected the employee manual to determine that an employee manual was utilized to document organizational policy statements and codes of conduct and to communicate entity values and behavioral standards to personnel.	No exceptions noted.
1.03	Policies and procedures require that employees sign an acknowledgment form upon hire indicating that they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.	Inspected the employee handbook acknowledgment form for a sample of employees hired during the period to determine that each employee sampled signed an acknowledgment form upon hire indicating that they had been given access to the employee manual and understood their responsibility for adhering to the policies and procedures contained within the manual.	No exceptions noted.
1.04	Management ensures that employees have adequate training to carry out their job responsibilities.	Inspected the training expenditures during the period and the departmental training materials available to employees to determine that employees had training to carry out their job responsibilities.	No exceptions noted.
1.05	A Board of Managers is in place to oversee management activities.	Inquired of the Legal Administrator regarding the Board of Managers to determine that a Board of Managers was in place to oversee management activities.	No exceptions noted.
		Observed the most recent Board of Managers meeting minutes to determine that a Board of Managers was in place and met to oversee management activities during the period.	No exceptions noted.

HR MANAGEMENT

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that employee onboarding and offboarding procedures are utilized to ensure compliance with company policies and security practices.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.01	Background screenings are performed for employee candidates as a component of the hiring process.	Inspected the background investigation procedures and the completed background screening for a sample of employees hired during the period to determine that background screenings were performed for employee candidates as a component of the hiring process for each employee sampled.	No exceptions noted.
2.02	Drug screening tests are performed for employee candidates as a component of the hiring process.	Inspected the completed drug screening test for a sample of employees hired during the period to determine that drug screening tests were performed for employee candidates as a component of the hiring process for each employee sampled.	No exceptions noted.
2.03	Employees must sign a confidentiality statement upon hire agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.	Inspected the signed confidentiality statement for a sample of employees hired during the period to determine that each employee sampled signed a confidentiality statement upon hire agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.	No exceptions noted.
2.04	Employees, customers, and vendors undergo orientation prior to accessing a data center to help ensure that security and safety requirements are communicated.	Inquired of the Director of IT Compliance regarding communication of security and safety requirements to determine that employees, customers, and vendors underwent orientation prior to accessing a data center to ensure that security and safety requirements were communicated.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the security orientation materials to determine that security orientation included the following topics: • **Building perimeter security** • **Customer and guest access** • **Mantraps, turn-styles, and other physical barriers to entry** • **Fire safety** • **Security points of contact for emergencies**	**No exceptions noted.**
		Inspected the information security policy and the information security policy acknowledgment for a sample of employees hired during the period to determine that each employee sampled acknowledged their responsibilities with respect to information security and safety requirements upon hire.	No exceptions noted.
		Inspected the completed security orientation form for a sample of employees hired during the period to determine that each employee sampled underwent orientation upon hire.	No exceptions noted.
		Inspected the arc flash safety procedures and the completed arc flash training roster for a sample of employees hired during the period to determine that each employee sampled completed electrical system safety training upon hire.	No exceptions noted.
		Inspected the physical access request evidence for a sample of customers and vendors granted access during the period to determine that each customer and vendor sampled underwent orientation prior to accessing the data centers.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.05	Access to buildings and systems is revoked for employees upon resignation or termination.	Inquired of the Director of IT Compliance regarding termination of access privileges to determine that access to buildings and corporate systems was revoked for employees upon resignation or termination.	No exceptions noted.
		Inspected the separation clearance checklist and the user account listing for the badge access system and for a sample of in-scope systems and employees terminated during the period to determine that access was revoked upon resignation or termination for each in-scope system and employee sampled.	No exceptions noted.

PHYSICAL SECURITY

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

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
3.01	Security policies and procedures are documented to guide employee activities for granting, controlling, and monitoring physical access to the data centers.	Inspected the security policies and procedures to determine that security policies and procedures were documented and included guidance regarding employee activities for granting, controlling, and monitoring physical access to the data centers.	No exceptions noted.
3.02	Security policies and procedures are documented to guide customer, vendor, and guest activities for access control.	Inspected the security policies and procedures to determine that security policies and procedures were documented to guide customer, vendor, and guest activities for access to the data centers.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
3.03	A security badge policy is in place to define the appropriate use of the badge access cards.	Inspected the access control procedures to determine that a security badge policy was in place that defined the appropriate use of the badge access cards.	No exceptions noted.
	Badge Access Management		
3.04	The ability to create, modify, or delete user badge access privileges to the facilities is restricted to user accounts accessible by authorized personnel.	Inspected the badge system configurations and the listing of user accounts with the ability to create, modify, or delete user badge access privileges with the assistance of the Director of IT Compliance to determine that the ability to create, modify, or delete user badge access privileges to the facilities was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
3.05	A full review of employee and customer access privileges is performed on a semi-annual basis.	Inquired of the Director of IT Compliance regarding the semi-annual access review to determine that a full review of employee and customer access privileges was performed on a semi-annual basis.	No exceptions noted.
		Inspected the results of the most recent user access review to determine that a review of employee and customer access privileges was performed during the six months preceding the end of the period.	No exceptions noted.
3.06	Badge access card privileges are assigned to users using predefined access zones to help ensure that access privileges are consistently assigned based on job responsibilities and/or where customer equipment is located.	Inspected the badge access card privileges and zone definition configurations to determine that badge access card privileges were assigned to users using predefined access zones to ensure that access privileges were consistently assigned based on job responsibilities and/or where customer equipment was located.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
3.07	Badge access privileges assigned to terminated employees are revoked within 24 hours as a component of the employee termination process.	Inquired of the Director of IT Compliance regarding termination of badge access to determine that badge access privileges assigned to terminated employees were revoked within 24 hours as a component of the employee termination process.	No exceptions noted.
		Inspected the separation clearance checklist and the badge access user account listing for a sample of employees terminated during the period to determine that badge access privileges were revoked within 24 hours for each employee sampled.	No exceptions noted.
	Building Perimeter and Initial Access		
3.08	The building perimeters for the facilities include a minimum set of physical barriers that include: • Fences / walls • Entrance gates controlled by guards or card access	Observed the building perimeter for the in-scope facilities to determine that each facility included the following physical barriers: • Fences / walls • Entrance gates controlled by guards or card access	No exceptions noted.
3.09	Security personnel utilize surveillance cameras to monitor the main entrance to the data centers and identify visitors and contractors prior to granting them access into the facilities.	Observed the data center entrance process for the in-scope facilities to determine that security personnel utilized surveillance cameras to monitor the main entrance to the data centers and identified visitors and contractors prior to granting them access into the facilities.	No exceptions noted.
3.10	Visitors are required to present a picture identification card, which is either retained or digitally scanned, and must be escorted by authorized individuals before being granted access to the facilities.	Inquired of the SVP of SecOps regarding the visitor sign-in process to determine that visitors were required to present a picture identification card that would be either retained or digitally scanned, and would be escorted by authorized individuals before being granted access to the facilities and while in the facilities.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Observed the visitor sign-in process for the in-scope facilities with the assistance of the SVP of SecOps to determine that visitors were required to present a picture identification card, which was either retained or digitally scanned, and were escorted by authorized personnel during the sign-in process.	No exceptions noted.
3.11	Physical access to the data center is documented and approved by the employee's manager prior to access being granted.	Inspected the physical access request approval for a sample of employees and contractors granted access during the period to determine that physical access to the data center was documented and approved by the employee's manager prior to access being granted for each employee and contractor sampled.	No exceptions noted.
	Access Within the Facilities		
3.12	Personnel at the facilities are distinguished as being either an employee, customer, or contractor with a functioning color-coded badge access card or a visitor with a non-functioning visitor badge.	Inquired of the SVP of SecOps regarding access to the in-scope facilities to determine that personnel at the facilities were distinguished as one of the following: • Employee with badge access card • Customer with badge access card • Contractor with badge access card • Visitor with non-functioning visitor badge	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Observed personnel within the in-scope facilities to determine that personnel were distinguished by the following badge access card designations: • **Employees – red colored badge access cards and lanyards – Security had red-colored badges and black lanyards** • **Customers – blue colored badge access cards and lanyards** • **Contractors – black colored badge access cards and lanyards** • **Visitors – yellow colored badge access cards labeled "visitor" with yellow lanyards**	**No exceptions noted.**
3.13	Personnel and authorized customers and contractors are required to enter a mantrap where they must provide the badge access card and a biometric credential prior to being granted access to the secure interior of the data centers.	Observed the data center entrance process for the in-scope facilities to determine that personnel and authorized customers and contractors were required to enter a mantrap where they provided a badge access card and a biometric credential prior to being granted access to the secure interior of the data centers.	No exceptions noted.
3.14	Personnel and authorized visitors are required to provide badge access cards and biometric identification for both entry and exit of interior doors.	Observed the interior door entry and exit access process for the in-scope facilities to determine that personnel and authorized visitors were required to provide badge access cards and biometric identification for both entry and exit of interior doors.	No exceptions noted.
3.15	Visitors without badge access cards are required to be escorted by authorized employees while within the facilities.	Observed the visitor access procedures for the in-scope facilities with the assistance of the SVP of SecOps to determine that visitors without badge access cards were escorted by authorized employees while within the facilities.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the access control policy to determine that procedures were in place to require visitors to be escorted by authorized employees while within the facilities.	No exceptions noted.
3.16	Physical access to customer cages is documented and approved by the customer prior to access being granted.	Inspected the physical access request approval to customer cages for a sample of vendors and customers granted access during the period to determine that physical access to the customer cages was documented and approved by the customer prior to access being granted for each sample selected.	No exceptions noted.
	Monitoring and Incident Management		
3.17	Activity logs of certain physical movements within the facilities are monitored and maintained.	Inquired of the SVP of SecOps regarding physical access monitoring to determine that activity logs for movement within the facilities were logged and that personnel reviewed logs on an ad hoc basis in response to incidents and alarms.	No exceptions noted.
		Inspected example activity logs recorded during the period to determine that the following attributes for physical movements within the facilities were captured and maintained during the period: • Date / time • Event • Badge access card details • Device	No exceptions noted.
3.18	Digital surveillance video cameras record activities at facility entrances, the building perimeters, and other areas within the facilities.	Observed the digital surveillance video camera dashboard within the security command center at the in-scope facilities to determine that digital surveillance video cameras recorded activities at facility entrances, the building perimeters, and other areas within the facilities.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
3.19	Digital surveillance video camera recordings are archived, allowing the capability for ad hoc investigations.	Inspected the digital surveillance recording configurations to determine that digital surveillance video camera recordings were archived, allowing the capability for ad hoc investigations.	No exceptions noted.
3.20	The data centers are monitored 24 hours per day with the use of motion-sensitive digital surveillance cameras, alarms, and motion detectors.	Observed the monitoring tools at the in-scope facilities to determine that the data centers were monitored 24 hours per day with the use of motion-sensitive digital surveillance cameras, alarms, and motion detectors.	No exceptions noted.
3.21	Security personnel monitor access to facility entrances and manage visitor access 24 hours per day.	Observed the security personnel at the security command center for the in-scope facilities to determine that security personnel monitored access to facility entrances and managed visitor access.	No exceptions noted.
		Inspected the most recent master shift schedule for security personnel across the in-scope facilities to determine that security personnel were staffed to monitor access to the facilities on a 24 hour per day basis during the period.	No exceptions noted.
3.22	Security personnel utilize an incident reporting system to document physical security incidents.	Inspected the listing of physical security incidents during the period within the incident reporting system to determine that security personnel utilized an incident reporting system to document physical security incidents during the period.	No exceptions noted.
3.23	The physical security hardware (e.g., monitoring servers, DVRs) is secured behind locked server racks and physical cages.	Observed the secured server racks and physical cages for the in-scope facilities to determine that the physical security hardware was secured behind locked server racks and physical cages.	No exceptions noted.

ENVIRONMENTAL SECURITY

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

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	Fire Detection and Suppression		
4.01	Fire safety procedures are documented to guide employee, contractor, and visitor activities for fire prevention, detection, and response.	Inspected the fire safety procedures to determine that fire safety procedures were documented and included guidance regarding employee, contractor, and visitor activities for fire prevention, detection, and response.	No exceptions noted.
4.02	The data center facilities are protected by fire detection and suppression controls that include the following: • Fire alarms • Dry-pipe water sprinklers • Fire detectors • Hand-held fire extinguishers • Smoke and heat sensors	**Observed the fire detection and suppression devices at the in-scope facilities to determine that the data center facilities were protected by fire detection and suppression controls that included the following:** • **Fire alarms** • **Dry-pipe water sprinklers** • **Fire detectors** • **Hand-held fire extinguishers** • **Smoke and heat sensors**	**No exceptions noted.**
4.03	Dual-interlock (pre-action) dry pipe water sprinklers, which require an occurrence of pressure loss (heat) and a secondary smoke detection event to release water into the pipes, are located throughout the data centers.	Inquired of the SVP of Security regarding fire suppression at the in-scope facilities to determine that dual-interlock (pre-action) dry pipe water sprinklers were located throughout the data centers.	No exceptions noted.
		Observed the pre-action dry pipe water sprinklers at the in-scope facilities to determine that dual-interlock (pre-action) dry pipe water sprinklers were located throughout the data centers.	No exceptions noted.
4.04	The business process director obtains inspection reports as evidence that the fire suppression systems undergo maintenance inspections on a quarterly basis.	Inspected the fire suppression system inspection report for a sample of quarters during the period for the in-scope facilities to determine that the fire suppression systems underwent maintenance inspections for each quarter sampled.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
4.05	The business process director obtains inspection reports as evidence that the fire alarm systems undergo maintenance inspections on a quarterly basis.	Inspected the fire alarm system inspection report for a sample of quarters during the period for the in-scope facilities to determine that the fire alarm systems underwent maintenance inspections for each quarter sampled.	No exceptions noted.
4.06	The business process director obtains inspection tags as evidence that the hand-held fire extinguishers undergo maintenance inspections on an annual basis.	Observed the inspection tag for a sample of hand-held fire extinguishers at the in-scope facilities to determine that each hand-held fire extinguisher sampled underwent maintenance inspections during the period.	No exceptions noted.
	Temperature and Humidity		
4.07	Critical infrastructure policies and procedures are documented to establish responsibility and procedures for power and environmental systems management.	Inspected the critical infrastructure policies and procedures to determine that critical infrastructure policies and procedures were documented to establish responsibility and procedures for power and environmental systems management.	No exceptions noted.
4.08	An inspection matrix guides the frequency of inspection for critical infrastructure including power and cooling systems.	Inspected the critical infrastructure maintenance matrix to determine that an inspection matrix was maintained that included guidance for the frequency of inspection for critical infrastructure including power and cooling systems.	No exceptions noted.
4.09	The data centers' temperature and humidity levels are systematically monitored. Operations personnel are notified via e-mail and text message when predefined minimum and maximum thresholds are exceeded.	Inquired of the SVP of SecOps regarding the monitoring of temperature and humidity levels at the in-scope facilities to determine that the data centers' temperature and humidity levels were systematically monitored and that operations personnel were notified via e-mail and text message when predefined minimum and maximum thresholds were exceeded.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the monitoring system configurations and example alerts generated during the period for the in-scope facilities to determine that the data centers' temperature and humidity levels were systematically monitored and that operations personnel were notified via e-mail and text message when predefined minimum and maximum thresholds were exceeded.	No exceptions noted.
4.10	The data centers are designed to optimize cool air flow and utilize redundant air conditioning units to keep infrastructure equipment at optimal temperatures.	Observed the redundant air conditioning units at the in-scope facilities to determine that the data centers utilized redundant air conditioning units.	No exceptions noted.
		Observed the server farm layout at the in-scope facilities with the assistance of the SVP of SecOps to determine that the data centers utilized thermal separate compartmentalization to pull warm air from behind sever racks and pull it up through centralized cooling towers.	No exceptions noted.
		Observed the cooling towers and associated pump skid at the in-scope facilities to determine that the data centers had devices in place to maintain climate control.	No exceptions noted.
4.11	The business process director obtains inspection reports as evidence that the air conditioning systems undergo maintenance inspection on a quarterly basis.	Inspected the air conditioning system inspection report for a sample of quarters during the period for the in-scope facilities to determine that the air conditioning systems underwent maintenance inspection for each quarter sampled.	No exceptions noted.
4.12	Internal personnel inspect and maintain the air conditioning systems on at least a quarterly basis to help ensure that they are functioning properly.	Inspected the air conditioning system inspection report for a sample of quarters during the period for the in-scope facilities to determine that internal personnel inspected and maintained the air conditioning systems for each quarter sampled.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	Power Failure and Surge Control		
4.13	The data centers provide uninterrupted power through the combined use of redundant diesel generators as well as multiple UPS systems.	Observed the power generators at the in-scope facilities to determine that redundant diesel power generators were in place to provide power in the event of a power outage.	No exceptions noted.
		Observed the UPS systems at the in-scope facilities to determine that the data centers were connected to multiple UPS systems to provide temporary electricity in the event of a power outage.	No exceptions noted.
4.14	Power levels are systematically monitored and configured to alert personnel when predefined minimum and maximum thresholds are exceeded.	Inspected the monitoring system configurations and an example alert generated during the period to determine that power levels were systematically monitored and configured to alert personnel when predefined minimum and maximum thresholds were exceeded.	No exceptions noted.
4.15	The business process director obtains inspection reports as evidence that the generators undergo maintenance inspections on a quarterly basis.	Inspected the generator inspection report for a sample of quarters during the period for the in-scope facilities to determine that the generators underwent maintenance inspections for each quarter sampled.	No exceptions noted.
4.16	Internal personnel perform preventative maintenance procedures on the generators on a quarterly basis.	Inspected the generator inspection report for a sample of quarters during the period for the in-scope facilities to determine that internal personnel performed preventative maintenance procedures on the generators for each quarter sampled.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
4.17	UPS systems undergo documented maintenance inspections on a semi-annual basis.	Inspected the most recent UPS system inspection report for the in-scope facilities to determine that the UPS systems underwent documented maintenance inspections during the six months preceding the end of the period for the following in-scope data center facilities: • LAS 2 • LAS 4 • LAS 5 • LAS 7 • LAS 8 • LAS 9 • LAS 10 • LAS 11 • LAS 12 • LAS 15 • RNO 1 • GRR 1 • ATL 1	**No exceptions noted.**
		Inspected the data center operations maintenance schedule and the go-live date of the RNO 2 data center facility with the assistance of the VP of Data Center Operations and determined that there were no UPS maintenance inspections required for RNO 2 during the period since the systems were newly installed; therefore, no testing of operating effectiveness was performed.	
4.18	The data centers contain two distinct electrical connections to the electrical company's substation.	Inquired of the SVP of SecOps regarding electrical connectivity for the in-scope facilities to determine that the data centers contained two distinct electrical connections to the electrical company's substation.	No exceptions noted.
		Observed the power connections at the in-scope facilities to determine that the data centers had a redundant electrical connection to the electric company's substation.	No exceptions noted.

LOGICAL SECURITY

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that logical access to network infrastructure is restricted to authorized personnel.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
5.01	Documented logical security policies are in place to guide personnel in areas that include, but are not limited to, the following: • Acceptable usage • Password management • User access management	**Inspected the logical security policies to determine that documented logical security policies were in place to guide personnel in areas that included the following:** • **Acceptable usage** • **Password management** • **User access management**	**No exceptions noted.**
5.02	Network infrastructure devices restrict user access to Internet communication sessions originating from a predefined list of IP addresses.	Inspected the network infrastructure device configurations for a sample of network infrastructure devices to determine that each network infrastructure device sampled restricted user access to Internet communication sessions originating from a predefined list of IP addresses.	No exceptions noted.
5.03	Users communicate with network infrastructure devices via an SSH program to help ensure that communication sessions are encrypted using a cryptographic hash function.	Inquired of the Director of IT Compliance regarding logical access to network infrastructure to determine that users communicated with network infrastructure devices via an SSH program to ensure that communication sessions were encrypted using a cryptographic hash function.	No exceptions noted.
		Inspected the network infrastructure device configurations for a sample of network infrastructure devices to determine that communication sessions for each network infrastructure device sampled were encrypted using a cryptographic hash function.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
5.04	Network infrastructure devices are programmed to end a communication session after a predefined period of user inactivity.	Inspected the network device infrastructure configurations for a sample of network infrastructure devices to determine that each network infrastructure device sampled was programmed to end a communication session after a predefined period of user inactivity.	No exceptions noted.
5.05	A centralized authentication system is utilized to authenticate users accessing network infrastructure devices.	Inspected the centralized authentication system configurations for a sample of network infrastructure devices to determine that a centralized authentication system was utilized to authenticate users accessing each network infrastructure device sampled.	No exceptions noted.
5.06	Access to the centralized authentication system requires the use of a unique username and password.	Inspected the centralized authentication system user account listing and authentication configurations to determine that access to the centralized authentication system required the use of a unique username and password.	No exceptions noted.
5.07	Authentication parameters for the centralized authentication system are derived from the corporate network domain controller.	Inspected the centralized authentication system configurations to determine that authentication parameters for the centralized authentication system were derived from the corporate network domain controller.	No exceptions noted.
5.08	The network domain is configured to enforce the following user account and password controls: • Password minimum length • Password expiration intervals • Password complexity • Password history • Invalid password account lockout threshold	Inspected the network domain user account listing and authentication configurations to determine that the network domain was configured to enforce the following user account and password controls: • Password minimum length • Password expiration intervals • Password complexity • Password history • Invalid password account lockout threshold	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
5.09	The ability to access and administer network infrastructure is restricted to user accounts accessible by authorized personnel.	Inspected the network infrastructure administrator user account listing with the assistance of the Director of IT Compliance to determine that the ability to access and administer network infrastructure was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
5.10	The centralized authentication system is configured to log events that include, but are not limited to, the following: • Successful logins • Failed logins • Administrator commands executed during an active session IT management reviews central authentication system event logs on an ad hoc basis.	**Inquired of the Director of IT Compliance regarding the review of the centralized authentication system logs to determine that IT management reviewed central authentication system event logs on an ad hoc basis during the period.**	**No exceptions noted.**
		Inspected the centralized authentication system logging configurations and example logs generated during the period to determine that the centralized authentication system was configured to log the following events: • Successful logins • Failed logins • Administrator commands executed during an active session	No exceptions noted.

NETWORK MONITORING AND PROBLEM MANAGEMENT

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

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
6.01	Documented network monitoring and problem management procedures are in place to guide personnel in identifying, investigating, and resolving customer infrastructure problems.	Inspected the network monitoring and problem management procedures to determine that documented network monitoring and problem management procedures were in place to guide personnel in identifying, investigating, and resolving customer infrastructure problems.	No exceptions noted.
6.02	Routers are configured for redundancy such that if one fails, network connectivity is still available to customers.	Inspected the router redundancy configurations for a sample of routers to determine that each router sampled was configured for redundancy such that if one failed, network connectivity was still available to customers.	No exceptions noted.
6.03	Network monitoring applications are utilized to monitor network devices and are configured to notify operations personnel via e-mail when predefined events occur on the network.	Inspected the network monitoring application configurations and example alerts generated during the period to determine that network monitoring applications were utilized to monitor network devices and were configured to notify operations personnel via e-mail when predefined events occurred on the network.	No exceptions noted.
6.04	A dedicated NOC is staffed 24 hours per day to respond to customer inquiries, support issues, and incidents.	Inquired of the SVP of SecOps regarding customer support to determine that a dedicated NOC was staffed 24 hours per day to respond to customer inquiries, support issues, and incidents.	No exceptions noted.
		Inspected the NOC staffing schedule and the employee time report for a sample of weeks during the period to determine that the NOC was staffed 24 hours per day for each week sampled.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
6.05	Operations personnel utilize a ticketing system to track the status of incidents and service disruptions.	Inspected the ticketing system dashboard and the incident ticket for a sample of incidents that occurred during the period to determine that operations personnel utilized a ticketing system to track the status of incidents and service disruptions for each incident sampled.	No exceptions noted.
6.06	Operations personnel record information regarding incidents and service disruptions in an incident ticket as a component of the customer support process, that includes, but is not limited to, the following: • Date and time of the incident • Problem type • Description of event • Correspondence with customers • Resolution details	Inspected the incident ticket for a sample of incidents that occurred during the period to determine that operations personnel recorded information regarding incidents and service disruptions in an incident ticket as a component of the customer support process that included the following for each incident sampled: • Date and time of the incident • Problem type • Description of event • Correspondence with customers • Resolution details	No exceptions noted.
6.07	Operations personnel configure priority ratings for tickets created by the ticketing system depending on urgency and impact levels.	Inspected the ticketing system mapping and filter configurations to determine that priority ratings for tickets created by the ticketing system were configured depending on urgency and impact levels.	No exceptions noted.

CUSTOMER SUPPORT

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that dedicated customer support personnel are in place to handle customer communications and that issues are escalated according to predefined procedures.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
7.01	Documented customer support procedures are in place to guide personnel in customer support activities that include, but are not limited to, the following: • Ticketing • Communication to customers • Customer complaint resolution • Maintenance • Event response	**Inspected the customer support procedures to determine that documented customer support procedures were in place to guide personnel in customer support activities that included the following:** • Ticketing • Communication to customers • Customer complaint resolution • Maintenance • Event response	**No exceptions noted.**
7.02	Documented customer support procedures are in place to guide personnel in verifying that customer inquiries and support requests are initiated by authorized customer personnel.	Inspected the customer support procedures to determine that documented customer support procedures were in place to guide personnel in verifying that customer inquiries and support requests were initiated by authorized personnel.	No exceptions noted.
7.03	A dedicated NOC is staffed 24 hours per day to respond to customer inquiries, support issues, and incidents.	Inquired of the SVP of SecOps regarding customer support to determine that a dedicated NOC was staffed 24 hours per day to respond to customer inquiries, support issues, and incidents.	No exceptions noted.
		Inspected the NOC staffing schedule and the employee time report for a sample of weeks during the period to determine that the NOC was staffed 24 hours per day for each week sampled.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
7.04	Operations personnel utilize a ticketing system to track the status of incidents and service disruptions.	Inspected the ticketing system dashboard and the incident ticket for a sample of incidents that occurred during the period to determine that operations personnel utilized a ticketing system to track the status of incidents and service disruptions for each incident sampled.	No exceptions noted.
7.05	Operations personnel record information regarding incidents and service disruptions in an incident ticket as a component of the customer support process, that includes, but is not limited to, the following: • Date and time of the incident • Problem type • Description of event • Correspondence with customers • Resolution details	**Inspected the incident ticket for a sample of incidents that occurred during the period to determine that operations personnel recorded information regarding incidents and service disruptions in an incident ticket as a component of the customer support process that included the following for each incident sampled:** • Date and time of the incident • Problem type • Description of event • Correspondence with customers • Resolution details	**No exceptions noted.**
7.06	The ticketing system is configured for NOC personnel to perform real-time monitoring of open tickets that have not been addressed within predefined time frames based on the severity of the ticket.	Inspected the ticketing system notification configurations to determine that the ticketing system was configured for NOC personnel to perform real-time monitoring of open tickets that had not been addressed within the predefined time frames based on the severity of the ticket.	No exceptions noted.

CUSTOMER PROVISIONING

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

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
8.01	Documented policies and procedures are in place to guide IT and operations personnel in the customer provisioning process.	Inspected the customer provisioning policies and procedures and the customer provisioning thank you template to determine that documented policies and procedures were in place to guide IT and operations personnel in the customer provisioning process.	No exceptions noted.
8.02	Operations personnel require a customer service agreement to be executed in order to begin the implementation process.	Inspected the executed service agreement for a sample of customers provisioned during the period to determine that a customer service agreement was executed prior to operations personnel beginning the implementation process for each customer sampled.	No exceptions noted.
8.03	A completed engineering document and client contact form is required prior to the provisioning process that includes, but is not limited to, the following: • Contact information • Network connectivity requirements • Network redundancy requirements • Customer cabinet layout	Inquired of the Manager of IT Compliance regarding the customer implementation process to determine that a completed engineering document and client contact form was obtained prior to the provisioning process that included the following: • Contact information • Network connectivity requirements • Network redundancy requirements • Customer cabinet layout	No exceptions noted.
		Inspected the completed provisioning questionnaire for a sample of customers provisioned during the period to determine that a completed provisioning questionnaire was obtained for each customer sampled.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
8.04	Members of the IT and operations groups conduct a new customer welcome call with new customers to review requested settings to help ensure that the services to be provisioned match the customer's expectations.	Inquired of the Director of IT Compliance regarding the customer implementation process to determine that members of the IT and operations groups conducted a new customer welcome call with new customers to review requested settings to ensure that the services to be provisioned matched the customer's expectations.	No exceptions noted.
		Inspected evidence of a customer welcome call for a sample of customers provisioned during the period to determine that members of the IT and operations groups conducted a new customer welcome call with each customer sampled.	No exceptions noted.

SECTION 5

OTHER INFORMATION PROVIDED BY SWITCH

DISASTER AVOIDANCE

Nevada provides an ideal setting for data center facilities as the area is considered a "safe-zone" from natural disasters. Nevada also has a highly sophisticated power grid and is a prime gateway for data flow from the West Coast to the East Coast.

NEVADA POWER GRID

Why Nevada for Power?

Nevada's alternative energy capacity is unique in the United States with a rare and rich blend of solar, wind and geothermal resources. These resources and capacities set Nevada apart as an ideal state for sustainable energy. Specifically, Nevada offers the nation's leading solar radiance and temperate windows, perfect for photovoltaic and solar concentration solutions.[1] Additionally, Nevada's wind capacity alone has been estimated as capable of supporting 60 percent of the state's needs.[2] Lastly, Nevada's geothermal solutions are among the oldest in the nation and growing. As the Las Vegas Sun has reported, "Nevada is poised to overtake California as the American geothermal energy leader. All of this is undergirded with natural gas lines that run through Las Vegas, Carson City, and Reno to supply the major population centers. In short, Nevada is perfectly poised to provide clean, affordable, and renewable energy.

Nevada's electrical grid is also robust and resilient. Nevada's climate, predictable and moderate weather patterns, and lack of natural disasters make Nevada ideal for electrical distribution and transmission and telecommunications networks. While other states are constantly required to repair, refurbish, and rebuild electrical systems to compete with corrosion and severe weather, Nevada's grids enjoy the mild seasonality and humidity of Nevada's temperate deserts.

Energy sustainability and self-sufficiency are becoming increasingly important for mission critical services. As the world begins to stir out of the global recession, industrialized nations' need for oil to fuel their factories and transportation and economies will continue to increase. The United States is not yet self-sufficient when it comes to oil. Month after month, the United States still imports about two-thirds of the oil consumed and 70 percent of that use is for transportation fuel. Nevada's unique renewable energy capabilities offer environmental responsibility and economic stability in the face of national dependence on fluctuating oil prices.

Where Does Switch Power Come from in Nevada?

Switch is committed to supporting its operations with 100 percent renewable and clean power, including power from Switch Station 1 and Switch Station 2, to provide 180 megawatts of photovoltaic generation. Securing 100 percent of Switch's energy from renewable sources is a central part of Switch's strategy and commitment to being planet friendly.

[1] See data provided by NREL, available at:
http://interestingenergyfacts.blogspot.com/2008/04/us-solar-energy-map.html

[2] See data provided by NREL, available at:
http://apps2.eere.energy.gov/wind/windexchange/wind_resource_maps.asp?stateab=nv

SWITCH, LTD.

SOC 2 REPORT

FOR

SWITCH COLOCATION SERVICES

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

OCTOBER 1, 2022, TO SEPTEMBER 30, 2023

Attestation and Compliance Services

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

If the 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 I

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To Switch, Ltd.:

Scope

We have examined Switch, Ltd.'s ("Switch" or the "service organization") accompanying description of its Switch Colocation Services system, in Section 3, throughout the period October 1, 2022, to September 30, 2023, (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 October 1, 2022, to September 30, 2023, to provide reasonable assurance that Switch'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).*

The information included in Section 5, "Other Information Provided by Switch" is presented by Switch management to provide additional information and is not a part of the description. Information about Switch's disaster avoidance and Nevada power grid 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 Switch's service commitments and system requirements based on the applicable trust services criteria.

Service Organization's Responsibilities

Switch 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 Switch's service commitments and system requirements were achieved. Switch has provided the accompanying assertion, in Section 2, ("assertion") about the description and the suitability of design and operating effectiveness of controls stated therein. Switch 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.
- 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 are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement, including the Code of Professional Conduct established by the AICPA and the International Ethics Standards Board for Accountants' Code of Ethics for Professional Accountants.

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 Switch's Colocation Services system that was designed and implemented throughout the period October 1, 2022, to September 30, 2023, in accordance with the description criteria;

b. the controls stated in the description were suitably designed throughout the period October 1, 2022, to September 30, 2023, to provide reasonable assurance that Switch's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the period; and

c. the controls stated in the description operated effectively throughout the period October 1, 2022, to September 30, 2023, to provide reasonable assurance that Switch's service commitments and system requirements were achieved based on the applicable trust services criteria.

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 Switch; user entities of Switch's Colocation Services system during some or all of the period October 1, 2022, to September 30, 2023, business partners of Switch subject to risks arising from interactions with

the Switch 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;
- 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
November 8, 2023

SECTION 2

MANAGEMENT'S ASSERTION

MANAGEMENT'S ASSERTION

We have prepared the accompanying description of Switch's Colocation Services system, in Section 3, throughout the period October 1, 2022, to September 30, 2023, (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 Switch Colocation Services system that may be useful when assessing the risks arising from interactions with Switch's system, particularly information about system controls that Switch 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).*

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

a. the description presents Switch's Colocation Services system that was designed and implemented throughout the period October 1, 2022, to September 30, 2023, in accordance with the description criteria;

b. the controls stated in the description were suitably designed throughout the period October 1, 2022, to September 30, 2023, to provide reasonable assurance that Switch'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

c. the controls stated in the description operated effectively throughout the period October 1, 2022, to September 30, 2023, to provide reasonable assurance that Switch's service commitments and system requirements would be achieved based on the applicable trust services criteria.

SECTION 3

DESCRIPTION OF THE SYSTEM

OVERVIEW OF OPERATIONS

Company Background

Switch is a technology infrastructure ecosystem corporation whose core business is the design, construction, and operation of data centers. Founded in 2000 and headquartered in Las Vegas, Nevada, Switch is built on the intelligent and sustainable growth of the Internet. The Founder and CEO, Rob Roy, has developed more than 700 issued and pending patent claims covering data center designs that manifested into Switch data centers and technology solution ecosystems. Since the opening of their first colocation facility, Switch has delivered 100% uptime across their facilities. At Switch, every team member is driven to produce real results for their clients – technologically and financially. Switch data center ecosystems empower their clients with numerous options for innovation, economies of scale, risk mitigation, sustainability, and investment protection.

Company Profile

Switch's advanced data centers are the center of their platform and provide power densities that exceed industry averages with efficient cooling, while being powered by 100% renewable energy. Two of the Switch data centers are the only carrier-neutral colocation facilities in the world to be certified Tier IV Design, Tier IV Facility, and Tier IV Gold in Operational Excellence. While these certifications have been the highest classifications available in the industry, Switch is building their current facilities to their proprietary Tier 5 Platinum standards, which exceed Tier IV standards. Switch's platform has powerful network effects and nurtures a technology ecosystem that benefits its participants. Switch continues to further enhance these benefits as they innovate and expand their platform ecosystem. Switch currently has over 1,000 customers, including technology and digital media companies, cloud, and managed service providers, financial institutions, and telecommunications providers.

The growing nexus between Internet connectivity, Internet-based services, data and analytics, and the advancement of computational processing power is rapidly expanding the amount of data that enterprises can access and manage. At the same time, the Internet of Everything is exponentially expanding the available data sources, as utility grids, automobiles, aircraft, home appliances, wearable devices, and numerous other sources are all connecting to the Internet. The compute capacity necessary to manage and analyze this data is also advancing and demanding increasing amounts of power to operate. Switch believes that traditional technology infrastructure is not capable of supporting the growing wave of mission critical data and increasingly powerful IT equipment.

Switch presently owns and operates four primary campus locations, called Primes, which encompass fourteen colocation facilities with an aggregate of over 5.3 million gross square feet (GSF) of space. These facilities have approximately 470 megawatts (MW) of power available to them. Primes consist of The Core Campus in Las Vegas, Nevada; The Citadel Campus near Reno, Nevada; The Pyramid Campus in Grand Rapids, Michigan; and The Keep Campus in Atlanta, Georgia. Primes are strategically located in geographies that combine a low risk of natural disaster, favorable tax policies for customers deploying computing infrastructure, and low latency connectivity to major metropolitan markets, such as Los Angeles, San Francisco, Silicon Valley, Chicago, New York, Northern Virginia, and Miami. As a result, customers in these metropolitan markets can access Switch's colocation facilities while reducing exposure to higher taxes, higher cost of power, and higher risk of natural disaster that might be prevalent in other markets. Switch can also use their Switch Modular Optimized Design (MOD) technology to build single-user facilities and are actively pursuing opportunities to deploy this technology in a build-to-suit offering for their enterprise customers.

As additional locations and sectors within the four existing Prime campus locations are opened for Colocation Services, the same / similar controls tested within this report are implemented / in place.

Description of Services Provided

Physical Security

Exterior Barriers

From well-defined perimeters consisting of signage, blast walls, and gates, to clear avenues of approach and backup perimeter barriers, the first layer of physical security is extensive. Exterior walls are constructed of either steel reinforced poured concrete or masonry reinforced beyond building code requirements. Entry points are kept to a minimum and each exterior door is reinforced, alarmed, access-controlled, and viewed by two dedicated fixed cameras.

Interior Barriers and Customer Compartmentalization

Exterior doors lead into specially engineered mantraps built over fire corridor wall construction. The mantraps are sheeted with steel and seams are strapped by aluminum. Access points off the mantrap require additional multi-factor biometric authentication of the card holder and are controlled via a 24 hour per day security officer and mantrap relay logic. Each mantrap includes fixed cameras viewing each door.

Each customer space, whether it is a cage, cabinet, or suite, is individually locked, protected, and monitored. Additional security safeguards, such as mantraps, intrusion sensors, and surveillance cameras, can be added to these spaces at the customer's request.

Positive Access Control

Positive Access Control is the application of a two-fold access principle stemming from the questions, "Who are you? And why should we let you in?" When first granted access to the facility, a multi-step process is in place to determine identity and verify need for access. In addition to the metal walls, turnstiles, cameras, intercoms, and biometric readers, Switch's access control takes on further hardening by the Positive Access Control procedures deployed at the facilities. Positive Access Control requires that a proprietary 24 hours per day officer staffed security command center (SECOM) verifies that the person standing in the mantrap matches a file photo. After confirmation, the officer activates the second proximity and biometric reader for use.

The access process is further continued with periodic access audits performed each shift by the shift supervisor. Customer audits are conducted monthly by the campus security manager. A complete audit of personnel with access to the facilities is conducted by the Security Director on a semi-annual basis.

Surveillance

Surveillance equipment for the facilities follows an elite standard set by a board-certified security professional. Fixed cameras are high-resolution color (520 lines) or digital high definition (HD) with automatic low light switching, capable of viewing up to 0.1 lux. Pan / tilt / zoom (PTZ) cameras are used on the exterior and areas of sensitivity. Video is digitally recorded at common interchange format (CIF) resolution at 15 images per second (IPS) upon motion at 4CIF 30 IPS upon operator command or at select zones requiring enhanced video. Video is retained for 100 +/- 10 days.

Switch deploys active surveillance with on-staff officers operating the camera system 24 hours per day. Camera operators use the Identify, Observe and Understand (IOU) methodology. The IOU methodology includes constant monitoring, use of cameras for detection, and a usable video product for investigations.

Sensors

Detectors are used around the property and provide early warning for perimeter and sensitive area intrusion. Sensor types include infrared motion, ultrasonic motion, photoelectric motion, electromechanical, internal lock, and seismic. These sensors are installed based on the environment or protection needs.

Security Team

Switch has a proprietary SECOM fully staffed 24 hours per day. Security staff members are hired with military and law enforcement security experience and must complete an extensive training period, which includes security system instruction, procedure and policy instruction, and non-lethal weapon training. The Security Academy was developed in accordance with the current American Society for Industrial Security (ASIS) International Guideline on

Private Security Officer Selection and Training (ASIS GDL PSO-2010) and the 90-day field training officer (FTO) program. A security supervisor oversees each shift and reports to the campus security manager. Security supervisors are required to attend a Security Management course, and officers in management positions are required to be active members of ASIS International.

Please refer to the following link for related pictures and detailed information: http://www.switch.com.

Infrastructure Operations (Environmental Security)

Switch employs the latest advanced environmental controls to protect the systems of its customers as well as operating with energy efficiency. These systems are managed and monitored by the Data Center Operations (DCO) and Energy Management Systems (EMS) teams.

Fire Protection

Fire protection includes fire, smoke, and heat detection monitored 24 hours per day. Sensors are located throughout the data centers and provide alerts to physical security personnel and a third-party monitoring company for response. Data center areas are protected by aspirating smoke detectors, which are programmed to identify smoke in the incipit stage.

The data centers are equipped with dual-interlock pre-action dry pipe sprinklers. Specifically, these dual-interlock pre-action sprinklers require both a smoke detection event and the activation of sprinklers to release water into the pipes. This allows for quick response to a fire with a lower risk of water damage in the case of a smaller fire or false alarm.

Heating, Ventilation, and Cooling (HVAC)

Switch utilizes advanced, patented techniques starting with a custom-designed thermal separate compartment in facility or (t-scif) air-flow system. This airflow system pulls the warm air away from customer systems into a separate compartment. The warm air is taken out of the core SUPERNAP facility designed for 74 high-grade Switch-designed and patented TSC-600 and TSC-1000 HVAC units which are physically adjacent to the data center, each containing six types of air conditioning systems. Within the data centers, areas where warm or hot air travels are marked in red.

Please refer to the following link for related pictures and detailed information: http://www.switch.com.

Power Management

Switch utilizes multiple in-bound connections from electricity providers. Tri-redundant power systems, which balance dual in-bound power connections across three sources of power, optimize the power utilization. Power is currently provided in redundancy through the use of uninterruptable power supply (UPS) devices which are fed by generators across the campuses. Power distribution units are managed and secured to prevent tampering. Power cabling within the data center is color-coded for quick and succinct identification of circuits and to assist with troubleshooting.

Please refer to the following link for related pictures and detailed information: http://www.switch.com.

Support for Colocation Services

Switch maintains dedicated support for its customers 24 hours per day via the Network Operations Center (NOC). NOC and engineering staff are available to assist with network troubleshooting and provide "hands-on" services to support customers.

NOC representatives follow defined procedures to facilitate confirmation of identification, customer communication of unexpected events that may impact their systems, customer authorization (only authorized customer representatives can open a service request), and functional escalation for customer service requests and incidents. NOC representatives monitor customer inquiries, support issues, and incidents on a real-time basis. Issues are documented in the Living Data Center (LDC) ticketing system and tracked to resolution.

The ticketing system / customer relationship management (CRM) system contains a complete purchased product hierarchy, installed equipment, and the physical and logical infrastructure layouts of individual customer solutions.

The complete history of customer service requests and incidents are recorded in the ticketing system. Customer-specific information is handled confidentially through permission-access levels in the ticketing system and access to customer infrastructures. Documented procedures are in place for the monitoring of customer support operations. Furthermore, volume analysis, response times, and procedural adherence are monitored to help ensure customer obligations are met.

Network Management and Monitoring (Logical Security)

Since Switch has no logical access to any customer's equipment or data, each customer is responsible for its own network security. Switch manages the network connectivity to the Internet via its multiple providers. Switch's core routers are managed by the network engineering team and monitored by the NOC 24 hours per day. Routers are configured for high availability in active-active mode such that if one fails or connectivity is lost, network traffic is diverted accordingly.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Switch designs business processes and procedures to meet its objectives for its Colocation Services. Those objectives are based on the service commitments that Switch makes to user entities, the laws and regulations that govern the provisioning of Colocation Services, and the financial, operational, and compliance requirements that Switch has established for the services.

Principal Service Commitments

Security and availability commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Switch makes the following principal service commitments to their customers:

- Make available Switch's colocation and/or other services to customers for the service term
- Establish, implement, and maintain commercially reasonable industry standards designed to protect the customers' equipment
- Provide services to customers in accordance with the service level goals
- Make available Switch's colocation space 24 hours per day, 7 days a week
- Offer service to customers regarding network availability, network latency, packet delivery, and power delivery
- Provide 99.99% availability of the Switch network in any calendar month
- Provide 100% power availability
- Availability of HVAC capacity to maintain temperatures in the area around the colocation space

System Requirements

Switch establishes operational requirements that support the achievement of the principal service commitments, relevant laws and regulations, and other system requirements. These requirements include account and password management processes, vulnerability assessment and remediation processes, and employee background screening and security awareness training. Additional requirements are the necessary system change management procedures to support the requisite authorization, documentation, testing, and approval of system changes.

System requirements are communicated in Switch's policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired, trained, and managed. Switch also has procedures in place to review documentation from third-party providers to ensure

that they are in compliance with security and availability policies. Commitments and requirements of Switch are documented in customer contracts and are updated and signed upon any changes in the practices.

In accordance with Switch'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

The scope of this report is limited to the Colocation Services for the following facilities:

- Las Vegas, Nevada
  - Las Vegas 2 (LAS 2)
  - Las Vegas 4 (LAS 4)
  - Las Vegas 5 (LAS 5)
  - Las Vegas 7 (LAS 7)
  - Las Vegas 8 (LAS 8)
  - Las Vegas 9 (LAS 9)
  - Las Vegas 10 (LAS 10)
  - Las Vegas 11 (LAS 11)
  - Las Vegas 12 (LAS 12)
  - Las Vegas 15 (LAS 15)
- Reno, Nevada
  - Reno 1 (RNO 1)
  - Reno 2 (RNO 2)
- Grand Rapids, Michigan
  - Grand Rapids 1 (GRR 1)
- Atlanta, Georgia.
  - Atlanta 1 (ATL 1)

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 system components described below.

[Intentionally Blank]

Infrastructure and Software

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

Primary Infrastructure			
Production System	**Business Function Description**	**Operating System Platform**	**Physical Location**
The Living Data Center (LDC) Application	Overall environmental conditions monitoring as well as ticketing system capability to track incidents and resolutions.	Linux	Las Vegas, Nevada Reno, Nevada Grand Rapids, Michigan Atlanta, Georgia
Microsoft Active Directory Domain	Network domain supporting internal systems applicable to the Colocation Services.	Windows	
Cisco Border and Private Routers	Network devices in place to direct traffic and filter unauthorized inbound network traffic from the Internet.	Cisco Internetwork Operating System (IOS)	
Honeywell Badge Access System	Physical access control supporting the Colocation Services at the Las Vegas, Reno, and Grand Rapids facilities that was decommissioned during November 2022. The in-scope facilities using Honeywell transitioned to C-Cure prior to the end of November 2022.	Windows	
C-Cure Badge Access System	Physical access control supporting the Colocation Services at the Las Vegas, Reno, Grand Rapids, and Atlanta facilities.		

In addition, Switch utilizes CrowdStrike antivirus software for antivirus protection for the Windows production servers and workstations. Furthermore, Switch utilizes Milestone Video Management System (VMS) for managing the security cameras for the interior and exterior of the data centers.

People

Switch utilizes specific functional areas of operations that support the scope of this review that include, but are not limited to, the following:

- Executive Management – responsible for overseeing company-wide activities, establishing and accomplishing goals, and overseeing objectives.
- Security Operations (SecOps) department – responsible for monitoring and protecting the facility from unauthorized access, damage, and interference.
- Network Operations (NetOps) department – responsible for implementation of product development and optimization, client implementation, and technical operations.
- Data Center Operations (DCO) – responsible for monitoring and maintaining critical infrastructure including electrical and cooling infrastructure. Also responsible for preparing customer environment (cage, cabinet) and performing everyday maintenance of the facility.
- Energy Management Systems (EMS) department – responsible for monitoring and maintaining critical infrastructure including power equipment and infrastructure.
- Network Engineering department – responsible for managing network architecture.
- Facilities Services department – responsible for providing user entities with assistance before and after the initial sale by providing information, guidance, and continued support.

- Human Resources (HR) department – responsible for HR policies, practices, and processes with a focus on key HR department delivery areas (e.g., talent acquisitions, employee retention, compensation, employee benefits, performance management, employee relations, development, and employee-related incidents and investigations).
- Legal department – responsible for legal and regulatory issues involving corporate risk and corporate compliance.

Procedures

Access, Authentication, and Authorization

In order to gain access to the firewalls and routers, a user must authenticate with a user account and password via a secure shell (SSH) program to help ensure that the sessions are encrypted. The routers may only be managed from an internal network as SSH is not running on the public portion of the routers. SSH sessions are programmed to terminate a session after a predefined period of inactivity.

The network engineering team manages the security administration of the firewalls and routers and is required to authenticate through a terminal access controller access-control system plus (TACACS+) server which allows for individualized user account access, administration, and logging. These unique user accounts are defined by the TACACS+ server and are configured to authenticate using the corporate network domain.

The network domain is configured to enforce password requirements that include minimum length, expiration intervals, complexity, minimum history, and invalid account lockout threshold. Additionally, the operating system and badge access system are also configured to inherit credentials from the corporate network domain. Encrypted VPNs are required for remote access to production and enforce two-factor authentication.

Predefined access groups are employed within the network domain, operating system, badge access system, VPN system, and centralized authentication system to limit access based on job responsibilities. Additionally, administrator access to the aforementioned systems is restricted to only those personnel responsible for those activities via user account permissions and group assignments. Management reviews employee access privileges on a semi-annual basis.

IT management has configured the network domain, operating system, badge access system, VPN system, firewalls, and centralized authentication system to log access related events. IT management reviews these logs on an ad hoc basis to determine if any suspicious or unauthorized activity has occurred.

Access Requests and Access Revocation

Upon hire, an employee's production system access is requested, communicated, and approved by the employee's manager. The system access request details the specific production systems and required levels of access privileges. When an employee ends their employment, a termination checklist is completed to document the offboarding procedures performed and production system access is revoked.

Physical Asset Disposal

Documented data retention and destruction policies and procedures are in place to define retention periods and destruction procedures for assets that are no longer needed. When technology assets reach the end of their useful life, they are sent to the local IT team for disposal. IT personnel securely erase storage media in accordance with data destruction policies and procedures. Depending on the level of sensitivity of data contained on equipment being destroyed, physical destruction may be required. Destruction of computer equipment is performed off-site by a third-party vendor which issues certificates of destruction to confirm the destruction.

Physical Security

Switch has implemented various physical security protocols to protect the business premises and information systems from unauthorized access. A badge access system is in place 24 hours per day to control access to the office. Predefined access groups are utilized to provide access depending on the individual's role and responsibilities. Physical access to the data center is documented and approved by the employee's manager prior to access being granted, while physical access to customer cages is documented and approved by the customer

prior to access being granted. Badge access attempts are logged by the system and are traceable to specific badge access cards. Management reviews employee and customer access privileges on a semi-annual basis. The ability to administer the badge access system is restricted to authorized security management personnel. If an individual who has physical access to the Switch facilities is terminated, security management personnel revoke the badge access privileges within 24 hours as a component of the termination process.

The building perimeters for the facilities include fences, walls, and entrance gates controlled by guards or card access. In addition, surveillance cameras are utilized by security personnel to monitor the main entrance to the facilities in order to identify visitors and contractors prior to granting access to the facilities. Visitors must present photo identification before being granted access to the facilities. Personnel at the facilities are distinguished as being an employee, customer, or contractor with a functioning color-coded badge access card or a visitor with a non-functioning visitor badge. Prior to being granted access to the secure interior of the data centers, personnel and authorized customers must enter a mantrap where they must scan the badge access card and provide biometric credentials. Personnel and authorized visitors are required to provide badge access cards and biometric identification for both entry and exit of interior doors. Visitors without badge access cards are required to be escorted by authorized employees while within the facilities.

Switch maintains and monitors activity logs of certain physical movements within the facilities on an as needed basis. Physical movements captured and monitored include date / time, event, badge access card details, and device. Digital surveillance cameras are in place to monitor the facility entrances, the building perimeters, and other areas within the facilities. Video surveillance captured by the camera system is archived allowing the capability for review as needed. The facilities are monitored 24 hours per day by security personnel with the use of motion-sensitive digital surveillance cameras, alarms, and motion detectors. The physical security hardware (e.g., monitoring servers, DVRs) is secured behind locked server racks and physical cages. An incident reporting system is utilized by security personnel to document any physical security incidents.

Environmental Security

Switch has implemented various environmental security protocols to protect the business premises and information systems from potential environmental issues. The Switch facilities are protected by fire detection and suppression equipment that includes fire alarms, dry-pipe water sprinklers, fire and smoke detectors, hand-held fire extinguishers, and smoke and heat sensors. On a quarterly basis, the fire detection and suppression equipment undergo an inspection from a third-party specialist to help ensure that the equipment is in proper working order. Hand-held fire extinguishers undergo maintenance inspections on an annual basis.

Management utilizes an environmental monitoring tool which is configured to systematically monitor the humidity and temperature levels within the Switch data centers. The system is configured to automatically send e-mail notifications to operations personnel when predefined thresholds are exceeded. An inspection matrix guides the frequency of inspection for critical infrastructure including power and cooling systems.

The data centers are designed to optimize cool air flow and utilize redundant air conditioning units to keep infrastructure equipment at optimal temperatures. On a quarterly basis, the air conditioning systems undergo an inspection from a third-party specialist to help ensure that the equipment is in proper working order. The facilities are equipped with multiple UPS systems and diesel generators to provide electricity in the event of a power outage. The data centers also contain two distinct electrical connections to the electrical company's substation. Utility power is run through the UPS battery systems so that customers receive clean, conditioned battery power. In the event that a loss of utility power occurs, the generators will engage and begin supplying power to the UPS systems. Whether it is from utility or generator power, each customer draws power from the UPS battery systems, ensuring smooth transitions from utility to generator and back again. On a semi-annual basis, UPS inspections are performed, and on a quarterly basis, generator inspections are performed to help ensure that the systems are in proper working order. Additionally, internal personnel perform preventative maintenance procedures on the UPS systems and generators on a quarterly basis.

Malicious Software Management

Windows production servers and workstations are configured with CrowdStrike antivirus software which is configured to scan for updates to antivirus definitions and update signatures on a real-time basis and has on-access scanning of executables and files.

Change Management

Infrastructure changes follow formal change control procedures to help ensure that only tested (when applicable) and authorized changes are implemented. Change control procedures include:

- Identification and recording of significant changes;
- Planning and testing of changes;
- Assessment of the potential impacts, including security impacts, of such changes;
- Formal approval procedure for proposed changes from system or business owners;
- Communication of change details to relevant persons; and
- Audit trail of changes.

Changes are documented in ticketing systems with requirements for specific mandatory fields to be completed to perform risk assessments and to enable effective coordination and communication within the change process. IT management will review the ticket and provide their approval or rejection based on the change request. Changes are required to be tested prior to being implemented and post implementation to help ensure there is no adverse effect or impact on the system. Change control documentation reflects an audit trail of the change including the date and time of change, reason for change, the name of the person making the change, and the person or persons who authorized the change.

The ability to implement infrastructure changes is restricted to user accounts granted permissions and group assignments assigned to authorized executive management, IT, and NetOps personnel. Change management meetings are held on a weekly basis to discuss and communicate the ongoing and upcoming infrastructure changes and projects affecting the system. Meeting minutes are retained and approval for upcoming changes by the Change Advisory Board are documented within the respective change request ticket.

Disaster Recovery

Business resiliency plans, including disaster recovery plans, and contingency plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event. The plans include roles and responsibilities, recovery time objectives (RTO), procedures for various scenarios, and task checklists in the event of an emergency. Additionally, disaster recovery tests are performed on an annual basis. The results of the annual disaster plan are recorded and tracked to identify and monitor potential threats to the critical infrastructure supporting the Colocation Services.

Ongoing Monitoring

The entity's IT security group monitors the security impact of emerging technologies, and the impact of applicable laws or regulations are considered by senior management. Ongoing monitoring consists of IT personnel receiving e-mail notifications and subscriptions, as well as following blogs to stay informed of the latest IT trends which could affect system security and availability. IT security personnel utilize a third-party utility to perform a vulnerability scan of the production servers on a monthly basis to identify threats and assess their potential impact to the production environment. Any security vulnerabilities that are identified are triaged by IT security personnel and monitored through resolution.

Capacity and Availability Monitoring

Switch has implemented an internally developed custom built application called SYSLOG to monitor the network devices' capacity and availability levels (e.g., central processing unit (CPU) levels, uptime, etc.) and alert operations personnel when predefined thresholds have been met. Switch uses an enterprise monitoring tool to log and monitor network availability and security incidents.

On-call personnel are notified via e-mail by SYSLOG of availability issues that exceed predefined thresholds on monitored network devices. The NOC is staffed on a 24 hour a day on-call basis to respond to availability issues. Additionally, operations meetings are held on a weekly basis to review availability trends and availability forecasts as compared to system commitments.

Incident Response

The network infrastructure is monitored 24 hours per day by NOC technicians to assist with network issues and to respond to customer inquiries and incidents. Management has implemented procedures to guide NOC technicians in identifying and responding to network related incidents, as well as incident response and escalation procedures in the event that an event is detected, to provide timely and consistent communication to the business and customers.

A proprietary ticketing system, LDC, was developed and is utilized to handle network related issues in order to manage, track, and respond to network issues until resolution. When an issue is detected, NOC technicians will examine the issue and create a ticket to assign priority level on a scale (1-5) based on the urgency and impact of the incident to the business and/or the customer, and to determine predefined timelines to resolve the issue. If the ticket is not responded to within a predefined timeline based on its severity, the ticketing system is configured to notify NOC technicians of the open ticket until the ticket is addressed. Incidents identified by customers can be communicated to the NOC by phone, e-mail, or on the LDC portal.

If the issue cannot be resolved within the predefined timeline, escalation procedures have been implemented for the assigned NOC technician to notify the responsible department and/or vendor through a predetermined set of contacts. Once the affected departments have been notified of the issue, e-mail updates are sent out to the business or customers on an as needed basis until the issue is resolved. Once the issue is fixed, the NOC technician will update the support ticket with full details of the issue resolution and close the ticket. Additionally, management meetings are held on a biweekly basis to discuss incidents and corrective measures to help ensure that incidents are resolved.

Data

Badge access logs and video surveillance recordings are a key component of the Colocation Services provided by Switch. The logs and recordings are reviewed on a real-time basis by SECOM and retained for forensic purposes. Customer data was not included in the scope of this examination as Switch is not responsible for the administration or maintenance of customer systems or data.

Significant Changes During the Period

The RNO 2 data center facility was operational as of May 1, 2023. The test of controls at the facility only apply to the facility's dates of operation during the specified reporting period of May 1, 2023, to September 30, 2023, for the RNO 2 data center facility.

Subservice Organizations

No subservice organizations were applicable to the scope of this examination whose controls were necessary, in combination with controls at Switch, to provide reasonable assurance that Switch's service commitments and system requirements were achieved.

CONTROL ENVIRONMENT

The control environment at Switch is the foundation for the other areas of internal control. It sets the tone of the organization and influences the control consciousness of its personnel. The components of the control environment factors include the integrity and ethical values, management's commitment to competence, its organizational structure, the assignment of authority and responsibility, and the oversight and direction provided by the Board of Managers 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 Switch's control environment, affecting the design, administration, and monitoring of other components.

Integrity and ethical behavior are the product of Switch's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct. Specific control activities that Switch has implemented in this area are described below:

- An employee manual is utilized to document organizational policy statements and codes of conduct and communicate entity values and behavioral standards to personnel.
- Policies and procedures require that employees sign an acknowledgment form indicating that they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
- Employees must sign a confidentiality statement agreeing not to disclose proprietary or confidential information, including customer information, to unauthorized parties.
- Background screenings are performed for employee candidates as a component of the hiring process.
- Drug screening tests are performed for employee candidates as a component of the hiring process.
- As security is core to Switch's services, employees and contractors are required to attend security orientation and awareness training as a component of the hiring process and on an ongoing basis.

Board of Managers and Executive Management Oversight

Switch's control consciousness is influenced significantly by its Owners and Board of Managers' participation. A Board of Managers is in place to oversee management activities and meets on a quarterly basis.

Organizational Structure and Assignment of Authority and Responsibility

Switch's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Switch's management believes that establishing a relevant organizational structure includes considering key areas of authority and responsibility and lines of reporting. Switch has developed an organizational structure suited to its needs. This organizational structure is based, in part, on its size and the nature of its activities.

Switch's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to business practices, knowledge and experience of key personnel, and resources provided for carrying out duties.

In addition, it includes policies and communications directed at ensuring that personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable. Organizational charts are in place to communicate key areas of authority, responsibility, and lines of reporting to personnel. The charts are communicated to employees and updated as needed.

Commitment to Competence

Switch management defines competence as the knowledge and skills necessary to accomplish tasks that define an employee's roles and responsibilities. Switch'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.

Management ensures employees have adequate training to carry out their job responsibilities. This includes Switch's self-developed Security Academy where security personnel undergo incremental training in facilities security as well as Switch's physical security processes and supporting technology.

Accountability

Switch's management philosophy and operating style 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. Specific control activities that Switch has implemented in this area are described below:

- Input and feedback are actively sought from and provided by Switch customers and partners.
- Management is periodically briefed on regulatory and industry changes affecting the services provided.
- Management meetings are held on a periodic basis to discuss operational issues.

Switch's HR policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities. Specific control activities that Switch has implemented in this area are described below:

- Management has established pre-hire screening procedures which are performed for employee candidates.
- New hire onboarding includes, but is not limited to, the following elements:
    - Verification that the employee has signed the employee agreement;
    - Verification that the employee has signed the confidentiality agreement;
    - Verification that the employee has signed an acknowledgment of receipt of employee handbook document; and
    - Verification that the employee has taken security training and signed an acknowledgment of such training.
- Management utilizes termination procedures which include, but are not limited to, the following elements:
    - Collection of company property;
    - Revocation of physical and system access rights; and
    - Signatures of each person that performs requisite tasks.
- Evaluations are performed for employees on an annual basis.

RISK ASSESSMENT

Security and risk management are of primary importance to Switch. Switch's management has placed into operation a risk assessment process to identify and manage risks that could affect the organization's ability to provide reliable Colocation Services for user entities. This process requires management to identify significant risks in their areas of responsibility and to implement sufficient measures to address those risks.

Objective Setting

Switch faces a variety of risks from external and internal sources, and a precondition to Switch's risk assessment methodology is the establishment of objectives, linked at different levels and internally consistent. Objectives are

set at the strategic level, establishing a basis for operations, reporting, and compliance objectives. Objectives are aligned with Switch's risk appetite, which drives risk tolerance levels.

More specific objectives flow from the entity's broad strategy. Entity-level objectives are linked and integrated with more specific objectives established for various "activities," such as sales, marketing, and operations, making sure they are consistent. These sub-objectives, or activity-level objectives, include establishing goals and may deal with product line, market, financing, and profit objectives.

By setting objectives at the entity and activity levels, Switch can identify success factors. Success factors exist for the entity, a business unit, a function, a department, or an individual. Objective setting enables management to identify measurement criteria for performance, with focus on success factors. Switch has established certain broad categories including:

- **Operations objectives – these pertain to effectiveness and efficiency of the operations, including performance and delivery goals and safeguarding resources against loss. They vary based on management's choices about structure and performance.**
- **Compliance objectives – these objectives pertain to adherence to laws and regulations to which Switch and their customers are subject. They are dependent on external factors, such as government and industry regulation.**

Risk Identification and Analysis

Regardless of whether an objective is stated or implied, Switch's risk assessment process considers risks that may occur. Switch has considered significant interactions between itself and relevant external parties and risks that could affect the organization's ability to provide reliable service to its user entities.

Switch's methodology for analyzing risks varies largely because many risks are difficult to quantify. Nonetheless, the process usually includes:

- Estimating the significance of a risk
- Assessing the likelihood (or frequency) of the risk occurring
- Considering how the risk should be managed (i.e., an assessment of what actions need to be taken)

Risk analysis includes identification of key business processes where potential exposures of some consequence exist. Once the significance and likelihood of risk have been assessed, management considers how the risk should be managed. This involves judgment based on assumptions about the risk, and reasonable analysis of costs associated with reducing the level of risk.

Necessary actions are taken to reduce the significance or likelihood of the risk occurring.

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, incentives, pressures, opportunities, attitudes, and rationalizations
- A disruption in information systems processing
- The quality of personnel hired, and methods of training utilized
- Changes in management responsibilities
- The nature of the entity's activities and employee accessibility to assets

The Switch risk assessment process focuses on supporting management decisions and responding to potential threats by assessing risks and identifying important decision factors. Executive management oversees risk management ownership and accountability. Senior management from different operational areas is involved in the risk identification process. Management identifies elements of business risk including threats, vulnerabilities, safeguards, and the likelihood of a threat, to determine the actions to be taken.

Potential for Fraud

The potential for fraud is considered 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 misappropriation 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. Documented policies and procedures are in place to guide personnel in identifying the potential for fraud as part of the risk assessment process. Additionally, the annual risk assessment considers the potential for fraud.

Risk Mitigation

Risk mitigation activities include the ability to identify, select, and develop activities that sufficiently meet the identified risks. However, the relative costs versus benefits should also be considered when determining the risk mitigation activities. The organization has documented policies and procedures to guide personnel throughout this process. The annual risk assessment and mitigation process also addresses risks arising from potential business disruptions.

Vendors and business partners are also considered during the annual risk assessment and mitigation process. Documented policies and procedures are in place to guide personnel in identifying risks associated with vendors and business partners as part of the risk assessment process. Monitoring procedures are also in place to ensure continual compliance by vendors and business partners. This includes reviewing vendor audit reports and/or security questionnaires at least annually.

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 Switch'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 Switch Colocation Services system.

INFORMATION AND COMMUNICATION SYSTEMS

Relevant Information

Carriers and Connectivity

Switch has direct connections to many of the national Internet backbones. Its specific carriers are:

- Atlantic Telenetwork (Comnet)
- 123net
- Arelion
- Astound
- AT&T
- ATT Michigan (Michigan Bell Telephone Company)
- Bandwidth Infrastructure Group (BIG)
- Casair
- CC Communications
- Charter
- Cogent
- Comcast
- Cox
- Crown Castle (formerly Wilcon)
- Everstream (formerly Comlink)
- Global Telecom & Technology (GTT)
- IX Reach
- Lumen
- Masergy
- Megaport
- Packet Fabric
- Parker Fiber
- Pacific Century CyberWorks (PCCW) Limited
- Roberts
- Sky Fiber
- Tata
- Telepacific
- Telia
- Time Warner Cable
- T-Mobile (formerly Sprint)
- US Signal
- Valley Electric (VEA)
- Verizon
- Windstream
- Zayo

Network Design

Data centers are connected diversely and redundantly by Switch-owned fiber. Every data center has multiple pathways to the other data centers to take advantage of a broad blend of multiple providers on two different autonomous systems. This design succeeds in being dynamic, robust, and diverse.

Customers who collocate in one of the Switch facilities are provided a number of different options for Internet connectivity. These range from single drops to multiple redundant drops. Redundancy to the customer is provided either by Border Gateway Protocol (BGP) or Hot Standby Routing Protocol (HSRP).

The network core is built upon a platform of carrier-class equipment which services Switch's user entities. The border routers are meshed together to the core to maximize the ability to transport data to the optimal provider. Conversely, by having multiple providers, a customer's data is received in a fast and efficient method. Customers have the ability to choose between BGP, HSRP, and single connection routing.

Switch extends its availability into Southern California to the prominent One Wilshire Building. This presence enables Switch to peer with more than 50 international telecommunications companies.

Communication

Switch has implemented various methods of communication to help ensure that employees understand their individual roles and responsibilities for Colocation Services and controls, and to help ensure that significant events are communicated. These methods include orientation and training programs for newly hired employees and the use of electronic mail messages to communicate time-sensitive messages and information. Managers also hold periodic staff meetings.

MONITORING

At the executive level, controls are monitored to consider whether they are operating as intended or require modification for changes in conditions. Switch's management performs monitoring activities to continuously assess the quality of internal control over time. Monitoring activities occur on a continuous basis and necessary corrective actions are taken as required to correct deviations from company policy and procedures. This process is accomplished through ongoing monitoring activities and separate evaluations.

Ongoing Monitoring and Separate Evaluations

The Switch management team conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through management meetings, customer conference calls, and informal notifications.

The Board of Managers reviews internal control performance metrics provided by management on an annual basis. Management's close involvement in the operations can identify significant variances from expectations regarding internal controls. Upper management immediately evaluates the specific facts and circumstances with any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in Switch's procedures or personnel. The goal of this process is to ensure legal and regulatory compliance, as well as to maximize the performance of Switch personnel.

Switch utilizes the LDC system for overall monitoring. The platform includes an incident ticketing system as well as real-time monitoring capabilities. With respect to the previously mentioned control activities, the following are key monitoring controls:

- Video surveillance for physical security;
- Physical access logs;
- Semi-annual customer access reviews;

- Motion detection sensors;
- Fire, smoke, and heat detection sensors;
- Temperature and humidity monitors monitored by critical infrastructure staff;
- Air flow sensors monitored by critical infrastructure staff;
- Network device health monitoring with real-time alerts sent to network operations staff; and
- Logical access logs identifying authorized, unauthorized, and administrative activities on key network devices and platforms.

Additionally, Switch has periodic security assessments in accordance with the Department of Homeland Security (DHS) Argonne model. Internal audits are performed on an annual basis to help ensure that internal controls are designed and operating effectively to achieve organizational objectives. The results of audits are reviewed by management to develop and implement corrective action plans for control weaknesses as needed.

Evaluating and Communicating Deficiencies

Deficiencies in an entity's internal control system surface from many sources, including the company's ongoing monitoring procedures, separate evaluations of the internal control system, and external parties. Management has developed protocols to help ensure that findings of internal control deficiencies are reported not only to the individual responsible for the function or activity involved, who is in the position to take corrective action, but also to at least one level of management above the directly responsible person. This process enables that individual to provide needed support or oversight for taking corrective action, and to communicate with others in the organization whose activities may be affected. Management evaluates the specific facts and circumstances related to deficiencies in internal control procedures and makes the decision for addressing deficiencies based on whether the incident was isolated or requires a change in the company's procedures or personnel.

COMPLEMENTARY CONTROLS AT USER ENTITIES

Switch's controls are designed to provide reasonable assurance that the principal service commitments and system requirements can be achieved without the implementation of complementary controls at user entities. As a result, complementary user entity controls are not required, or significant, to achieve the principal 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 Switch. The scope of the testing was restricted to the Switch Colocation Services system and its boundaries as defined in Section 3. Schellman conducted the examination testing over the period October 1, 2022, to September 30, 2023.

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.

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	Policies and procedures require that employees sign an acknowledgment form upon hire indicating that they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.	Inspected the employee handbook acknowledgment form for a sample of employees hired during the period to determine that each employee sampled signed an acknowledgment form upon hire indicating that they had been given access to the employee manual and understood their responsibility for adhering to the policies and procedures contained within the manual.	No exceptions noted.
CC1.1.2	Background screenings are performed for employee candidates as a component of the hiring process.	Inspected the background investigation procedures and the completed background screening for a sample of employees hired during the period to determine that background screenings were performed for employee candidates as a component of the hiring process for each employee sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.1.3	Drug screening tests are performed for employee candidates as a component of the hiring process.	Inspected the completed drug screening test for a sample of employees hired during the period to determine that drug screening tests were performed for employee candidates as a component of the hiring process for each employee sampled.	No exceptions noted.
CC1.1.4	Employees must sign a confidentiality statement upon hire agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.	Inspected the signed confidentiality statement for a sample of employees hired during the period to determine that each employee sampled signed a confidentiality statement upon hire agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.	No exceptions noted.
CC1.1.5	An employee sanction policy is in place that addresses remedial actions for lack of compliance with policies and procedures.	Inspected the code of conduct and business ethics 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.
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	The Board of Managers establishes and maintains a formal charter and set of bylaws which describes their responsibilities and oversight of management's internal control environment.	Inspected the corporate governance charter to determine that the Board of Managers established and maintained a formal charter and set of bylaws which described their responsibilities and oversight of management's internal control environment.	No exceptions noted.
CC1.2.2	External board members attest to their independence from management and objectivity in evaluations and decision making on an annual basis.	Inspected the listing of management members and the Board of Managers to determine that external board members attested to their independence from management and objectivity in evaluations and decision making during the period.	No exceptions noted.
CC1.2.3	Board of Managers establish performance measures, incentives, and other rewards for responsibilities at the entity, reflecting dimensions of performance and expected standards of conduct.	Inspected the Board of Managers meeting minutes for a sample of quarters during the period to determine that Board of Managers established performance measures, incentives, and other rewards for responsibilities at the entity, reflecting dimensions of performance and expected standards of conduct for each quarter sampled.	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	Board of Managers establish performance measures, incentives, and other rewards for responsibilities at the entity, reflecting dimensions of performance and expected standards of conduct.	Inspected the Board of Managers meeting minutes for a sample of quarters during the period to determine that Board of Managers established performance measures, incentives, and other rewards for responsibilities at the entity, reflecting dimensions of performance and expected standards of conduct for each quarter sampled.	No exceptions noted.
CC1.3.2	Organizational charts are in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel. These charts are communicated to employees and updated as needed.	Inquired of the Director of IT Compliance regarding the communication of organizational charts to employees to determine that organizational charts were in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel and that these charts were communicated to employees and updated as needed.	No exceptions noted.
		Inspected the organizational charts to determine that organizational charts were in place and communicated key areas of authority, responsibility, and lines of reporting.	No exceptions noted.
CC1.3.3	Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.	Inspected the position description for a sample of job positions to determine that each position sampled had a documented position description that defined the skills, responsibilities, and knowledge levels required.	No exceptions noted.
CC1.3.4	Management has assigned responsibility of the maintenance and enforcement of the security and availability policies and procedures to the members of the SecOps, DCO, and NetOps teams.	Inspected the information security management system scope document and security roles and responsibilities policy to determine that management assigned responsibility of the maintenance and enforcement of the security and availability policies and procedures to the members of the SecOps, DCO, and NetOps teams.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.4 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC1.4.1	New employee checklists are utilized to guide the hiring process and include verification that candidates possess the required qualifications to perform the duties as outlined in the job description.	Inspected the new employee checklist for a sample of employees hired during the period to determine that new employee checklists were utilized to guide the hiring process and included verification that candidates possessed the required qualifications to perform the duties as outlined in the job description for each employee sampled.	No exceptions noted.
CC1.4.2	New employee hiring procedures are in place to guide the hiring process and include verification that candidates possess the required qualifications to perform the duties as outlined in the job description.	Inspected the hiring policy to determine that new employee hiring procedures were in place to guide the hiring process and included verification that candidates possessed the required qualifications to perform the duties as outlined in the job description.	No exceptions noted.
CC1.4.3	Management ensures that employees have adequate training to carry out their job responsibilities.	Inspected the training expenditures during the period and the departmental training materials available to employees to determine that employees had training to carry out their job responsibilities.	No exceptions noted.
CC1.4.4	Employees, customers, and vendors undergo orientation prior to accessing a data center to help ensure that security and safety requirements are communicated.	Inquired of the Director of IT Compliance regarding communication of security and safety requirements to determine that employees, customers, and vendors underwent orientation prior to accessing a data center to ensure that security and safety requirements were communicated.	No exceptions noted.
		Inspected the security orientation materials to determine that security orientation included the following topics: • Building perimeter security • Customer and guest access • Mantraps, turn-styles, and other physical barriers to entry • Fire safety • Security points of contact for emergencies	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the information security policy and the information security policy acknowledgment for a sample of employees hired during the period to determine that each employee sampled acknowledged their responsibilities with respect to information security and safety requirements upon hire.	No exceptions noted.
		Inspected the completed security orientation form for a sample of employees hired during the period to determine that each employee sampled underwent orientation upon hire.	No exceptions noted.
		Inspected the arc flash safety procedures and the completed arc flash training roster for a sample of employees hired during the period to determine that each employee sampled completed electrical system safety training upon hire.	No exceptions noted.
		Inspected the physical access request evidence for a sample of customers and vendors granted access during the period to determine that each customer and vendor sampled underwent orientation prior to accessing the data centers.	No exceptions noted.
CC1.4.5	Employees are required to complete security awareness training on an annual basis to understand their obligations and responsibilities to comply with the corporate and business unit security policies.	Inspected evidence of security awareness training completion for a sample of employees to determine that each employee sampled completed security awareness training to understand their obligations and responsibilities to comply with the corporate and business unit security policies during the period.	No exceptions noted.
CC1.5 COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CC1.5.1	Organizational charts are in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel. These charts are communicated to employees and updated as needed.	Inquired of the Director of IT Compliance regarding the communication of organizational charts to employees to determine that organizational charts were in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel and that these charts were communicated to employees and updated as needed.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the organizational charts to determine that organizational charts were in place and communicated key areas of authority, responsibility, and lines of reporting.	No exceptions noted.
CC1.5.2	Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.	Inspected the position description for a sample of job positions to determine that each position sampled had a documented position description that defined the skills, responsibilities, and knowledge levels required.	No exceptions noted.
CC1.5.3	An employee sanction policy is in place that addresses remedial actions for lack of compliance with policies and procedures.	Inspected the code of conduct and business ethics 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.
CC1.5.4	Management formally documents an organization strategy and performance policy and updates it on an annual basis to align internal control responsibilities, performance measures, and incentives with company business objectives.	Inspected the security management recurring meeting calendar invitation, example meeting notes, and the information security policy to determine that management formally documented an organization strategy and performance policy and updated it to align internal control responsibilities, performance measures, and incentives with company business objectives during the period.	No exceptions noted.
CC1.5.5	Board of Managers establish performance measures, incentives, and other rewards for responsibilities at the entity, reflecting dimensions of performance and expected standards of conduct.	Inspected the Board of Managers meeting minutes for a sample of quarters during the period to determine that Board of Managers established performance measures, incentives, and other rewards for responsibilities at the entity, reflecting dimensions of performance and expected standards of conduct for each quarter sampled.	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	An information classification policy is formally documented that identifies information required to support the functioning of internal control and achievement of objectives and associated protection and access rights.	Inspected the information classification policy to determine that an information classification policy was formally documented that identified information required to support the functioning of internal control and achievement of objectives and associated protection and access rights.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.1.2	Network monitoring applications are utilized to monitor network devices and are configured to notify operations personnel via e-mail when predefined events occur on the network.	Inspected the network monitoring application configurations and example alerts generated during the period to determine that network monitoring applications were utilized to monitor network devices and were configured to notify operations personnel via e-mail when predefined events occurred on the network.	No exceptions noted.
CC2.1.3	Security personnel monitor access to facility entrances and manage visitor access 24 hours per day.	Observed the security personnel at the security command center for the in-scope facilities to determine that security personnel monitored access to facility entrances and managed visitor access.	No exceptions noted.
		Inspected the most recent master shift schedule for security personnel across the in-scope facilities to determine that security personnel were staffed to monitor access to the facilities on a 24 hour per day basis during the period.	No exceptions noted.
CC2.1.4	The data centers' temperature and humidity levels are systematically monitored. Operations personnel are notified via e-mail and text message when predefined minimum and maximum thresholds are exceeded.	Inquired of the SVP of SecOps regarding the monitoring of temperature and humidity levels at the in-scope facilities to determine that the data centers' temperature and humidity levels were systematically monitored and that operations personnel were notified via e-mail and text message when predefined minimum and maximum thresholds were exceeded.	No exceptions noted.
		Inspected the monitoring system configurations and example alerts generated during the period for the in-scope facilities to determine that the data centers' temperature and humidity levels were systematically monitored and that operations personnel were notified via e-mail and text message when predefined minimum and maximum thresholds were exceeded.	No exceptions noted.
CC2.1.5	Power levels are systematically monitored and configured to alert personnel when predefined minimum and maximum thresholds are exceeded.	Inspected the monitoring system configurations and an example alert generated during the period to determine that power levels were systematically monitored and configured to alert personnel when predefined minimum and maximum thresholds were exceeded.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.1.6	The entity's IT security group monitors the security impact of emerging technologies, and the impact of applicable laws and regulations are considered by senior management.	Inspected example security update e-mail notifications received during the period to determine that the entity's IT security group monitored the security impact of emerging technologies, and the impact of applicable laws and regulations were considered by senior management.	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	A system description is documented that includes the services provided, data, people, software, infrastructure, procedures, control environment, risk assessment, monitoring, and information and communication systems. The system description is communicated to internal and external users via the customer-facing website.	Inspected the customer-facing website to determine that a system description was documented that included services provided, data, people, software, infrastructure, procedures, control environment, risk assessment, monitoring, and information and communication systems and was communicated to internal and external users via the customer-facing website.	No exceptions noted.
CC2.2.2	A documented information security policy is in place to guide personnel in the entity's security and availability commitments and the associated system requirements. The policy is communicated to internal personnel via the intranet.	Inspected the information security policy available on the company intranet to determine that a documented information security policy was in place to guide personnel in the entity's security and availability commitments and the associated system requirements, and that the policy was communicated to internal personnel via the intranet.	No exceptions noted.
CC2.2.3	Employees are required to complete security awareness training on an annual basis to understand their obligations and responsibilities to comply with the corporate and business unit security policies.	Inspected evidence of security awareness training completion for a sample of employees to determine that each employee sampled completed security awareness training to understand their obligations and responsibilities to comply with the corporate and business unit security policies during the period.	No exceptions noted.
CC2.2.4	Policies and procedures require that employees sign an acknowledgment form upon hire indicating that they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.	Inspected the employee handbook acknowledgment form for a sample of employees hired during the period to determine that each employee sampled signed an acknowledgment form upon hire indicating that they had been given access to the employee manual and understood their responsibility for adhering to the policies and procedures contained within the manual.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.2.5	Documented escalation procedures for reporting security and availability incidents are provided to internal and external users to guide users in identifying and reporting failures, incidents, concerns, and other complaints.	Inspected the escalation procedures available on the company intranet and the customer-facing website to determine that documented escalation procedures for reporting security and availability incidents were provided to internal and external users to guide users in identifying and reporting failures, incidents, concerns, and other complaints.	No exceptions noted.
CC2.2.6	Change management meetings are held on a weekly basis to discuss and communicate the ongoing and upcoming projects that affect the system.	Inspected the recurring calendar meeting invitation, agenda, and minutes for a sample of weeks during the period to determine that change management meetings were held to discuss and communicate the ongoing and upcoming projects that affected the system for each week sampled.	No exceptions noted.
CC2.2.7	Management meetings are held on a biweekly basis to discuss incidents and corrective measures to help ensure that incidents are resolved.	Inquired of the Director of IT Compliance regarding management meetings to determine that management meetings were held on a biweekly basis to discuss incidents and corrective measures to ensure that incidents were resolved.	No exceptions noted.
		Inspected the management meeting minutes for a sample of weeks during the period to determine that management meetings were held to discuss incidents and corrective measures for each week sampled.	No exceptions noted.
CC2.2.8	Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.	Inspected the position description for a sample of job positions to determine that each position sampled had a documented position description that defined the skills, responsibilities, and knowledge levels required.	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	A system description is documented that includes the services provided, data, people, software, infrastructure, procedures, control environment, risk assessment, monitoring, and information and communication systems. The system description is communicated to internal and external users via the customer-facing website.	Inspected the customer-facing website to determine that a system description was documented that included services provided, data, people, software, infrastructure, procedures, control environment, risk assessment, monitoring, and information and communication systems and was communicated to internal and external users via the customer-facing website.	No exceptions noted.
CC2.3.2	The entity's security and availability commitments and the associated system requirements are documented in customer contracts.	Inspected the standard executed customer service agreement to determine that the entity's security and availability commitments and the associated system requirements were documented in customer contracts.	No exceptions noted.
CC2.3.3	Members of the IT and operations groups conduct a new customer welcome call with new customers to review requested settings to help ensure that the services to be provisioned match the customer's expectations.	Inquired of the Director of IT Compliance regarding the customer implementation process to determine that members of the IT and operations groups conducted a new customer welcome call with new customers to review requested settings to ensure that the services to be provisioned matched the customer's expectations.	No exceptions noted.
		Inspected evidence of a customer welcome call for a sample of customers provisioned during the period to determine that members of the IT and operations groups conducted a new customer welcome call with each customer sampled.	No exceptions noted.
CC2.3.4	Documented escalation procedures for reporting security and availability incidents are provided to internal and external users to guide users in identifying and reporting failures, incidents, concerns, and other complaints.	Inspected the escalation procedures available on the company intranet and the customer-facing website to determine that documented escalation procedures for reporting security and availability incidents were provided to internal and external 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
CC2.3.5	A completed engineering document and client contact form is required prior to the provisioning process that includes, but is not limited to, the following: • **Contact information** • **Network connectivity requirements** • **Network redundancy requirements** • **Customer cabinet layout**	**Inquired of the Manager of IT Compliance regarding the customer implementation process to determine that a completed engineering document and client contact form was obtained prior to the provisioning process that included the following:** • **Contact information** • **Network connectivity requirements** • **Network redundancy requirements** • **Customer cabinet layout**	**No exceptions noted.**
		Inspected the completed provisioning questionnaire for a sample of customers provisioned during the period to determine that a completed provisioning questionnaire was obtained for each customer sampled.	No exceptions noted.
CC2.3.6	A dedicated NOC is staffed 24 hours per day to respond to customer inquiries, support issues, and incidents.	Inquired of the SVP of SecOps regarding customer support to determine that a dedicated NOC was staffed 24 hours per day to respond to customer inquiries, support issues, and incidents.	No exceptions noted.
		Inspected the NOC staffing schedule and the employee time report for a sample of weeks during the period to determine that the NOC was staffed 24 hours per day for each week sampled.	No exceptions noted.
CC2.3.7	Operations personnel utilize a ticketing system to track the status of incidents and service disruptions.	Inspected the ticketing system dashboard and the incident ticket for a sample of incidents that occurred during the period to determine that operations personnel utilized a ticketing system to track the status of incidents and service disruptions for each incident sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.3.8	Operations personnel record information regarding incidents and service disruptions in an incident ticket as a component of the customer support process, that includes, but is not limited to, the following: • Date and time of the incident • Problem type • Description of event • Correspondence with customers • Resolution details	**Inspected the incident ticket for a sample of incidents that occurred during the period to determine that operations personnel recorded information regarding incidents and service disruptions in an incident ticket as a component of the customer support process that included the following for each incident sampled:** • Date and time of the incident • Problem type • Description of event • Correspondence with customers • Resolution details	**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	Information security objectives are established by management to align internal control responsibilities, performance, and incentives with company business objectives.	Inspected the information security management system scope document to determine that information security objectives were established by management to align internal control responsibilities, performance, and incentives with company business objectives.	No exceptions noted.
CC3.1.2	Documented procedures are in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process.	Inspected the risk assessment procedures to determine that documented procedures were in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process.	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	A systems inventory is maintained that includes physical devices and systems, virtual devices, software, data and data flows, external information systems, and organizational roles.	Inquired of the Director of IT Compliance regarding the risk assessment process to determine that a systems inventory was maintained that included physical devices and systems, virtual devices, software, data and data flows, external information systems, and organizational roles.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the most recent risk assessment to determine that a systems inventory was maintained that included physical devices and systems, virtual devices, software, data and data flows, external information systems, and organizational roles.	No exceptions noted.
CC3.2.2	Documented procedures are in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process.	Inspected the risk assessment procedures to determine that documented procedures were in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process.	No exceptions noted.
CC3.2.3	A formal risk assessment is performed on an annual basis. Risks that are identified are rated using a risk evaluation process and are formally documented, along with mitigation strategies, for management review.	Inspected the most recent risk assessment documentation to determine that a formal risk assessment was performed and that risks that were identified were rated using a risk evaluation process and were formally documented, along with mitigation strategies, for management review during the period.	No exceptions noted.
CC3.2.4	Developments in technology and the impact of applicable laws or regulations are considered by senior management as part of the annual risk assessment and IT security planning process.	Inquired of the Director of IT Compliance regarding the risk assessment and IT security planning process to determine that developments in technology and the impact of applicable laws or regulations were considered by senior management as part of the annual risk assessment and IT security planning process.	No exceptions noted.
		Inspected the most recent risk assessment documentation to determine that a risk assessment was performed that considered developments in technology and the impact of applicable laws or regulations during the period.	No exceptions noted.
CC3.2.5	The entity's IT security group monitors the security impact of emerging technologies, and the impact of applicable laws and regulations are considered by senior management.	Inspected example security update e-mail notifications received during the period to determine that the entity's IT security group monitored the security impact of emerging technologies, and the impact of applicable laws and regulations were considered by senior management.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.3 COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
CC3.3.1	Management performs a risk assessment on an annual basis that includes consideration of the potential for fraud.	Inspected the most recent risk assessment documentation to determine that management performed a risk assessment that included consideration of the potential for fraud during the period.	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	Developments in technology and the impact of applicable laws or regulations are considered by senior management as part of the annual risk assessment and IT security planning process.	Inquired of the Director of IT Compliance regarding the risk assessment and IT security planning process to determine that developments in technology and the impact of applicable laws or regulations were considered by senior management as part of the annual risk assessment and IT security planning process.	No exceptions noted.
		Inspected the most recent risk assessment documentation to determine that a risk assessment was performed that considered developments in technology and the impact of applicable laws or regulations during the period.	No exceptions noted.
CC3.4.2	The entity's IT security group monitors the security impact of emerging technologies, and the impact of applicable laws and regulations are considered by senior management.	Inspected example security update e-mail notifications received during the period to determine that the entity's IT security group monitored the security impact of emerging technologies, and the impact of applicable laws and 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	IT security personnel utilize a third-party utility to perform a vulnerability scan of the production servers on a monthly basis to identify threats and assess their potential impact to the production environment. Any security vulnerabilities that are identified are triaged by IT security personnel and monitored through resolution.	Inspected the vulnerability scan report and an example remediation ticket for a sample of months during the period to determine that IT personnel utilized a third-party utility to perform a vulnerability scan of the production servers to identify threats and assess their potential impact to the production environment and that security vulnerabilities that were identified were triaged by IT security personnel and monitored through resolution for each month sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC4.1.2	Documented policies and procedures are in place to guide personnel in defining the audit scope and performing the internal system audit process.	Inspected the internal audit policies and procedures to determine that documented policies and procedures were in place to guide personnel in defining the audit scope and performing the internal system audit process.	No exceptions noted.
CC4.1.3	Internal audits are performed on an annual basis to help ensure that internal controls are designed and operating effectively to achieve organizational objectives. The results of audits are reviewed by management to develop and implement corrective action plans for control weaknesses as needed.	Inquired of the Director of IT Compliance regarding internal audits to determine that internal audits were performed on an annual basis to ensure that internal controls were designed and operating effectively to achieve organizational objectives and that the results of audits were reviewed by management to develop and implement corrective action plans for control weaknesses as needed.	No exceptions noted.
		Inspected the most recent internal audit report to determine that internal audits were performed to ensure that internal controls were designed and operating effectively to achieve organizational objectives and that the results of audits were reviewed by management to develop and implement corrective action plans for control weaknesses during the period.	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	Internal audits are performed on an annual basis to help ensure that internal controls are designed and operating effectively to achieve organizational objectives. The results of audits are reviewed by management to develop and implement corrective action plans for control weaknesses as needed.	Inquired of the Director of IT Compliance regarding internal audits to determine that internal audits were performed on an annual basis to ensure that internal controls were designed and operating effectively to achieve organizational objectives and that the results of audits were reviewed by management to develop and implement corrective action plans for control weaknesses as needed.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the most recent internal audit report to determine that internal audits were performed to ensure that internal controls were designed and operating effectively to achieve organizational objectives and that the results of audits were reviewed by management to develop and implement corrective action plans for control weaknesses during the period.	No exceptions noted.
CC4.2.2	The Board of Managers reviews internal control performance metrics provided by management on an annual basis.	Inspected the most recent Board of Managers meeting minutes to determine that the Board of Managers reviewed internal control performance metrics provided by management during the period.	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 procedures are in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process.	Inspected the risk assessment procedures to determine that documented procedures were in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process.	No exceptions noted.
CC5.1.2	A formal risk assessment is performed on an annual basis. Risks that are identified are rated using a risk evaluation process and are formally documented, along with mitigation strategies, for management review.	Inspected the most recent risk assessment documentation to determine that a formal risk assessment was performed and that risks that were identified were rated using a risk evaluation process and were formally documented, along with mitigation strategies, for management review during the period.	No exceptions noted.
CC5.1.3	Badge access card privileges are assigned to users using predefined access zones to help ensure that access privileges are consistently assigned based on job responsibilities and/or where customer equipment is located.	Inspected the badge access card privileges and zone definition configurations to determine that badge access card privileges were assigned to users using predefined access zones to ensure that access privileges were consistently assigned based on job responsibilities and/or where customer equipment was located.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.1.4	Security personnel utilize surveillance cameras to monitor the main entrance to the data centers and identify visitors and contractors prior to granting them access into the facilities.	Observed the data center entrance process for the in-scope facilities to determine that security personnel utilized surveillance cameras to monitor the main entrance to the data centers and identified visitors and contractors prior to granting them access into the facilities.	No exceptions noted.
CC5.1.5	Personnel and authorized customers and contractors are required to enter a mantrap where they must provide the badge access card and a biometric credential prior to being granted access to the secure interior of the data centers.	Observed the data center entrance process for the in-scope facilities to determine that personnel and authorized customers and contractors were required to enter a mantrap where they provided a badge access card and a biometric credential prior to being granted access to the secure interior of the data centers.	No exceptions noted.
CC5.1.6	Personnel and authorized visitors are required to provide badge access cards and biometric identification for both entry and exit of interior doors.	Observed the interior door entry and exit access process for the in-scope facilities to determine that personnel and authorized visitors were required to provide badge access cards and biometric identification for both entry and exit of interior doors.	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	Control activities over technology are identified as part of the risk assessment process to support the achievement of objectives and are documented within the risk assessment.	Inquired of the Director of IT Compliance regarding the risk assessment process to determine that control activities over technology were identified as part of the risk assessment process to support the achievement of objectives and were documented within the risk assessment.	No exceptions noted.
		Inspected the risk assessment policy and the most recent risk assessment to determine that control activities over technology were identified as part of the risk assessment process to support the achievement of objectives and were documented within the risk assessment during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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	A documented information security policy is in place to guide personnel in the entity's security and availability commitments and the associated system requirements. The policy is communicated to internal personnel via the intranet.	Inspected the information security policy available on the company intranet to determine that a documented information security policy was in place to guide personnel in the entity's security and availability commitments and the associated system requirements, and that the policy was communicated to internal personnel via the intranet.	No exceptions noted.
CC5.3.2	An information classification policy is formally documented that identifies information required to support the functioning of internal control and achievement of objectives and associated protection and access rights.	Inspected the information classification policy to determine that an information classification policy was formally documented that identified information required to support the functioning of internal control and achievement of objectives and associated protection and access rights.	No exceptions noted.
CC5.3.3	Policies and procedures are in place to document organizational policy statements, codes of conduct, and communicate entity values and behavioral standards to personnel.	Inspected the code of conduct and business ethics to determine that policies and procedures were in place to document organizational policy statements, codes of conduct, and communicate entity values and behavioral standards to personnel.	No exceptions noted.
CC5.3.4	Policies and procedures require that employees sign an acknowledgment form upon hire indicating that they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.	Inspected the employee handbook acknowledgment form for a sample of employees hired during the period to determine that each employee sampled signed an acknowledgment form upon hire indicating that they had been given access to the employee manual and understood their responsibility for adhering to the policies and procedures contained within the manual.	No exceptions noted.
CC5.3.5	An employee sanction policy is in place that addresses remedial actions for lack of compliance with policies and procedures.	Inspected the code of conduct and business ethics 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.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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	A systems inventory is maintained that includes physical devices and systems, virtual devices, software, data and data flows, external information systems, and organizational roles.	Inquired of the Director of IT Compliance regarding the risk assessment process to determine that a systems inventory was maintained that included physical devices and systems, virtual devices, software, data and data flows, external information systems, and organizational roles.	No exceptions noted.
		Inspected the most recent risk assessment to determine that a systems inventory was maintained that included physical devices and systems, virtual devices, software, data and data flows, external information systems, and organizational roles.	No exceptions noted.
CC6.1.2	An information classification policy is formally documented that identifies information required to support the functioning of internal control and achievement of objectives and associated protection and access rights.	Inspected the information classification policy to determine that an information classification policy was formally documented that identified information required to support the functioning of internal control and achievement of objectives and associated protection and access rights.	No exceptions noted.
CC6.1.3	Access to the network domain requires the use of a unique username and password.	Inspected the network domain user account listing and authentication configurations to determine that access to the network domain required the use of a unique username and password.	No exceptions noted.
CC6.1.4	The network domain is configured to enforce the following user account and password controls: • Password minimum length • Password expiration intervals • Password complexity • Password history • Invalid password account lockout threshold	Inspected the network domain user account listing and authentication configurations to determine that the network domain was configured to enforce the following user account and password controls: • Password minimum length • Password expiration intervals • Password complexity • Password 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
CC6.1.5	Access to the operating system requires the use of a unique username and password.	Inspected the operating system user account listing and authentication configurations for a sample of production servers to determine that access to each server sampled required the use of a unique username and password.	No exceptions noted.
CC6.1.6	Authentication parameters for the operating system are derived from the corporate network domain controller.	Inspected the operating system authentication configurations for a sample of production servers to determine that authentication parameters were derived from the corporate network domain controller for each server sampled.	No exceptions noted.
CC6.1.7	Access to the badge access system requires the use of a unique username and password.	Inspected the badge access system user account listing and authentication configurations to determine that access to the badge access system required the use of a unique username and password.	No exceptions noted.
CC6.1.8	Authentication parameters for the badge access system are derived from the corporate network domain controller.	Inspected the badge access system authentication configurations to determine that authentication parameters for the badge access system were derived from the corporate network domain controller.	No exceptions noted.
CC6.1.9	Encrypted VPNs are required for remote access to production and enforce two-factor authentication.	Inspected the VPN encryption and authentication configurations to determine that encrypted VPNs were utilized for remote access to production and enforced two-factor authentication.	No exceptions noted.
CC6.1.10	A centralized authentication system is utilized to authenticate users accessing network infrastructure devices.	Inspected the centralized authentication system configurations for a sample of network infrastructure devices to determine that a centralized authentication system was utilized to authenticate users accessing each network infrastructure device sampled.	No exceptions noted.
CC6.1.11	Access to the centralized authentication system requires the use of a unique username and password.	Inspected the centralized authentication system user account listing and authentication configurations to determine that access to the centralized authentication system required the use of a unique username and password.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.1.12	Authentication parameters for the centralized authentication system are derived from the corporate network domain controller.	Inspected the centralized authentication system configurations to determine that authentication parameters for the centralized authentication system were derived from the corporate network domain controller.	No exceptions noted.
CC6.1.13	Administrative access privileges within the network domain are restricted to user accounts accessible by authorized personnel.	Inspected the network domain administrator user account listing with the assistance of the Director of IT Compliance to determine that administrative access privileges within the network domain were restricted to user accounts accessible by authorized personnel.	No exceptions noted.
CC6.1.14	Administrative access privileges within the operating system are restricted to user accounts accessible by authorized personnel.	Inspected the operating system administrator user account listing for a sample of production servers with the assistance of the Director of IT Compliance to determine that administrative access privileges were restricted to user accounts accessible by authorized personnel for each server sampled.	No exceptions noted.
CC6.1.15	The ability to create, modify, or delete user badge access privileges to the facilities is restricted to user accounts accessible by authorized personnel.	Inspected the badge system configurations and the listing of user accounts with the ability to create, modify, or delete user badge access privileges with the assistance of the Director of IT Compliance to determine that the ability to create, modify, or delete user badge access privileges to the facilities was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
CC6.1.16	Administrative access privileges within the VPN system are restricted to user accounts accessible by authorized personnel.	Inspected the VPN system administrator user account listing with the assistance of the Manager of IT Compliance to determine that administrative access privileges within the VPN system were restricted to user accounts accessible by authorized personnel.	No exceptions noted.
CC6.1.17	The ability to access and administer network infrastructure is restricted to user accounts accessible by authorized personnel.	Inspected the network infrastructure administrator user account listing with the assistance of the Director of IT Compliance to determine that the ability to access and administer network infrastructure was restricted to user accounts accessible by authorized personnel.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.1.18	Predefined security groups are utilized to assign role-based access privileges and restrict access to data to the network domain.	Inspected the network domain user account listing and role assignments to determine that predefined security groups were utilized to assign role-based access privileges and restrict access to data to the network domain.	No exceptions noted.
CC6.1.19	Predefined security groups are utilized to assign role-based access privileges and restrict access to data to the operating system.	Inspected the operating system user account listing and role assignments for a sample of production servers to determine that predefined security groups were utilized to assign role-based access privileges and restrict access to data for each server sampled.	No exceptions noted.
CC6.1.20	Predefined security groups are utilized to assign role-based access privileges and restrict access to data to the badge access system.	Inspected the badge access system user account listing and role assignments to determine that predefined security groups were utilized to assign role-based access privileges and restrict access to data to the badge access system.	No exceptions noted.
CC6.1.21	Predefined security groups are utilized to assign role-based access privileges and restrict access to data to the centralized authentication system.	Inspected the centralized authentication system user account listing and role assignments to determine that predefined security groups were utilized to assign role-based access privileges and restrict access to data to the centralized authentication system.	No exceptions noted.
CC6.1.22	Predefined security groups are utilized to assign role-based access privileges and restrict access to data to the VPN system.	Inspected the VPN system user account listing and role assignments to determine that predefined security groups were utilized to assign role-based access privileges and restrict access to data to the VPN system.	No exceptions noted.
CC6.1.23	A firewall system is in place to filter unauthorized inbound network traffic from the Internet.	Inspected the firewall system ruleset for a sample of in-scope firewalls to determine that each firewall system sampled was configured to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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	Department managers complete a new hire onboarding checklist prior to granting system access privileges to new employees.	Inquired of the Director of IT Compliance regarding the access provisioning process to determine that IT personnel required department managers to complete a new hire onboarding checklist prior to granting system access privileges to new employees.	No exceptions noted.
		Inspected the new hire onboarding checklist for a sample of employees hired during the period to determine that a new hire onboarding checklist was completed for each employee sampled.	No exceptions noted.
CC6.2.2	A full review of employee and customer access privileges is performed on a semi-annual basis.	Inquired of the Director of IT Compliance regarding the semi-annual access review to determine that a full review of employee and customer access privileges was performed on a semi-annual basis.	No exceptions noted.
		Inspected the results of the most recent user access review to determine that a review of employee and customer access privileges was performed during the six months preceding the end of the period.	No exceptions noted.
CC6.2.3	A completed engineering document and client contact form is required prior to the provisioning process that includes, but is not limited to, the following: • Contact information • Network connectivity requirements • Network redundancy requirements • Customer cabinet layout	Inquired of the Manager of IT Compliance regarding the customer implementation process to determine that a completed engineering document and client contact form was obtained prior to the provisioning process that included the following: • Contact information • Network connectivity requirements • Network redundancy requirements • Customer cabinet layout	No exceptions noted.
		Inspected the completed provisioning questionnaire for a sample of customers provisioned during the period to determine that a completed provisioning questionnaire was obtained for each customer sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.2.4	A termination checklist is completed, and access is revoked for employees as a component of the employee termination process.	Inspected the termination checklist for a sample of employees terminated during the period to determine that a termination checklist was completed as a component of the employee termination process for each employee sampled.	No exceptions noted.
		Inspected the user account listing for a sample of in-scope systems and employees terminated during the period to determine that access was revoked for each in-scope system and employee sampled.	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	Department managers complete a new hire onboarding checklist prior to granting system access privileges to new employees.	Inquired of the Director of IT Compliance regarding the access provisioning process to determine that IT personnel required department managers to complete a new hire onboarding checklist prior to granting system access privileges to new employees.	No exceptions noted.
		Inspected the new hire onboarding checklist for a sample of employees hired during the period to determine that a new hire onboarding checklist was completed for each employee sampled.	No exceptions noted.
CC6.3.2	A full review of employee and customer access privileges is performed on a semi-annual basis.	Inquired of the Director of IT Compliance regarding the semi-annual access review to determine that a full review of employee and customer access privileges was performed on a semi-annual basis.	No exceptions noted.
		Inspected the results of the most recent user access review to determine that a review of employee and customer access privileges was performed during the six months preceding the end of the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.3.3	A completed engineering document and client contact form is required prior to the provisioning process that includes, but is not limited to, the following: • **Contact information** • **Network connectivity requirements** • **Network redundancy requirements** • **Customer cabinet layout**	**Inquired of the Manager of IT Compliance regarding the customer implementation process to determine that a completed engineering document and client contact form was obtained prior to the provisioning process that included the following:** • **Contact information** • **Network connectivity requirements** • **Network redundancy requirements** • **Customer cabinet layout**	**No exceptions noted.**
		Inspected the completed provisioning questionnaire for a sample of customers provisioned during the period to determine that a completed provisioning questionnaire was obtained for each customer sampled.	No exceptions noted.
CC6.3.4	A termination checklist is completed, and access is revoked for employees as a component of the employee termination process.	Inspected the termination checklist for a sample of employees terminated during the period to determine that a termination checklist was completed as a component of the employee termination process for each employee sampled.	No exceptions noted.
		Inspected the user account listing for a sample of in-scope systems and employees terminated during the period to determine that access was revoked for each in-scope system and employee sampled.	No exceptions noted.
CC6.3.5	Administrative access privileges within the network domain are restricted to user accounts accessible by authorized personnel.	Inspected the network domain administrator user account listing with the assistance of the Director of IT Compliance to determine that administrative access privileges within the network domain were restricted to user accounts accessible by authorized personnel.	No exceptions noted.
CC6.3.6	Administrative access privileges within the operating system are restricted to user accounts accessible by authorized personnel.	Inspected the operating system administrator user account listing for a sample of production servers with the assistance of the Director of IT Compliance to determine that administrative access privileges were restricted to user accounts accessible by authorized personnel for each server sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.3.7	The ability to create, modify, or delete user badge access privileges to the facilities is restricted to user accounts accessible by authorized personnel.	Inspected the badge system configurations and the listing of user accounts with the ability to create, modify, or delete user badge access privileges with the assistance of the Director of IT Compliance to determine that the ability to create, modify, or delete user badge access privileges to the facilities was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
CC6.3.8	Administrative access privileges within the VPN system are restricted to user accounts accessible by authorized personnel.	Inspected the VPN system administrator user account listing with the assistance of the Manager of IT Compliance to determine that administrative access privileges within the VPN system were restricted to user accounts accessible by authorized personnel.	No exceptions noted.
CC6.3.9	The ability to access and administer network infrastructure is restricted to user accounts accessible by authorized personnel.	Inspected the network infrastructure administrator user account listing with the assistance of the Director of IT Compliance to determine that the ability to access and administer network infrastructure was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
CC6.3.10	Predefined security groups are utilized to assign role-based access privileges and restrict access to data to the network domain.	Inspected the network domain user account listing and role assignments to determine that predefined security groups were utilized to assign role-based access privileges and restrict access to data to the network domain.	No exceptions noted.
CC6.3.11	Predefined security groups are utilized to assign role-based access privileges and restrict access to data to the operating system.	Inspected the operating system user account listing and role assignments for a sample of production servers to determine that predefined security groups were utilized to assign role-based access privileges and restrict access to data for each server sampled.	No exceptions noted.
CC6.3.12	Predefined security groups are utilized to assign role-based access privileges and restrict access to data to the badge access system.	Inspected the badge access system user account listing and role assignments to determine that predefined security groups were utilized to assign role-based access privileges and restrict access to data to the badge access system.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.3.13	Predefined security groups are utilized to assign role-based access privileges and restrict access to data to the centralized authentication system.	Inspected the centralized authentication system user account listing and role assignments to determine that predefined security groups were utilized to assign role-based access privileges and restrict access to data to the centralized authentication system.	No exceptions noted.
CC6.3.14	Predefined security groups are utilized to assign role-based access privileges and restrict access to data to the VPN system.	Inspected the VPN system user account listing and role assignments to determine that predefined security groups were utilized to assign role-based access privileges and restrict access to data to the VPN system.	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	Security policies and procedures are documented to guide employee activities for granting, controlling, and monitoring physical access to the data centers.	Inspected the security policies and procedures to determine that security policies and procedures were documented and included guidance regarding employee activities for granting, controlling, and monitoring physical access to the data centers.	No exceptions noted.
CC6.4.2	Security policies and procedures are documented to guide customer, vendor, and guest activities for access control.	Inspected the security policies and procedures to determine that security policies and procedures were documented to guide customer, vendor, and guest activities for access to the data centers.	No exceptions noted.
CC6.4.3	A security badge policy is in place to define the appropriate use of the badge access cards.	Inspected the access control procedures to determine that a security badge policy was in place that defined the appropriate use of the badge access cards.	No exceptions noted.
CC6.4.4	The ability to create, modify, or delete user badge access privileges to the facilities is restricted to user accounts accessible by authorized personnel.	Inspected the badge system configurations and the listing of user accounts with the ability to create, modify, or delete user badge access privileges with the assistance of the Director of IT Compliance to determine that the ability to create, modify, or delete user badge access privileges to the facilities was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
CC6.4.5	A full review of employee and customer access privileges is performed on a semi-annual basis.	Inquired of the Director of IT Compliance regarding the semi-annual access review to determine that a full review of employee and customer access privileges was performed on a semi-annual basis.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the results of the most recent user access review to determine that a review of employee and customer access privileges was performed during the six months preceding the end of the period.	No exceptions noted.
CC6.4.6	Badge access card privileges are assigned to users using predefined access zones to help ensure that access privileges are consistently assigned based on job responsibilities and/or where customer equipment is located.	Inspected the badge access card privileges and zone definition configurations to determine that badge access card privileges were assigned to users using predefined access zones to ensure that access privileges were consistently assigned based on job responsibilities and/or where customer equipment was located.	No exceptions noted.
CC6.4.7	Badge access privileges assigned to terminated employees are revoked within 24 hours as a component of the employee termination process.	Inquired of the Director of IT Compliance regarding termination of badge access to determine that badge access privileges assigned to terminated employees were revoked within 24 hours as a component of the employee termination process.	No exceptions noted.
		Inspected the separation clearance checklist and the badge access user account listing for a sample of employees terminated during the period to determine that badge access privileges were revoked within 24 hours for each employee sampled.	No exceptions noted.
CC6.4.8	The building perimeters for the facilities include a minimum set of physical barriers that include: • Fences / walls • Entrance gates controlled by guards or card access	Observed the building perimeter for the in-scope facilities to determine that each facility included the following physical barriers: • Fences / walls • Entrance gates controlled by guards or card access	No exceptions noted.
CC6.4.9	Security personnel utilize surveillance cameras to monitor the main entrance to the data centers and identify visitors and contractors prior to granting them access into the facilities.	Observed the data center entrance process for the in-scope facilities to determine that security personnel utilized surveillance cameras to monitor the main entrance to the data centers and identified visitors and contractors prior to granting them access into the facilities.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.4.10	Visitors are required to present a picture identification card, which is either retained or digitally scanned, and must be escorted by authorized individuals before being granted access to the facilities.	Inquired of the SVP of SecOps regarding the visitor sign-in process to determine that visitors were required to present a picture identification card that would be either retained or digitally scanned, and would be escorted by authorized individuals before being granted access to the facilities and while in the facilities.	No exceptions noted.
		Observed the visitor sign-in process for the in-scope facilities with the assistance of the SVP of SecOps to determine that visitors were required to present a picture identification card, which was either retained or digitally scanned, and were escorted by authorized personnel during the sign-in process.	No exceptions noted.
CC6.4.11	Personnel at the facilities are distinguished as being either an employee, customer, or contractor with a functioning color-coded badge access card or a visitor with a non-functioning visitor badge.	Inquired of the SVP of SecOps regarding access to the in-scope facilities to determine that personnel at the facilities were distinguished as one of the following: • Employee with badge access card • Customer with badge access card • Contractor with badge access card • Visitor with non-functioning visitor badge	No exceptions noted.
		Observed personnel within the in-scope facilities to determine that personnel were distinguished by the following badge access card designations: • Employees – red colored badge access cards and lanyards – Security had red-colored badges and black lanyards • Customers – blue colored badge access cards and lanyards • Contractors – black colored badge access cards and lanyards • Visitors – yellow colored badge access cards labeled "visitor" with yellow lanyards	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.4.12	Personnel and authorized customers and contractors are required to enter a mantrap where they must provide the badge access card and a biometric credential prior to being granted access to the secure interior of the data centers.	Observed the data center entrance process for the in-scope facilities to determine that personnel and authorized customers and contractors were required to enter a mantrap where they provided a badge access card and a biometric credential prior to being granted access to the secure interior of the data centers.	No exceptions noted.
CC6.4.13	Personnel and authorized visitors are required to provide badge access cards and biometric identification for both entry and exit of interior doors.	Observed the interior door entry and exit access process for the in-scope facilities to determine that personnel and authorized visitors were required to provide badge access cards and biometric identification for both entry and exit of interior doors.	No exceptions noted.
CC6.4.14	Visitors without badge access cards are required to be escorted by authorized employees while within the facilities.	Observed the visitor access procedures for the in-scope facilities with the assistance of the SVP of SecOps to determine that visitors without badge access cards were escorted by authorized employees while within the facilities.	No exceptions noted.
		Inspected the access control policy to determine that procedures were in place to require visitors to be escorted by authorized employees while within the facilities.	No exceptions noted.
CC6.4.15	Activity logs of certain physical movements within the facilities are monitored and maintained.	Inquired of the SVP of SecOps regarding physical access monitoring to determine that activity logs for movement within the facilities were logged and that personnel reviewed logs on an ad hoc basis in response to incidents and alarms.	No exceptions noted.
		Inspected example activity logs recorded during the period to determine that the following attributes for physical movements within the facilities were captured and maintained during the period: • Date / time • Event • Badge access card details • Device	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.4.16	Digital surveillance video cameras record activities at facility entrances, the building perimeters, and other areas within the facilities.	Observed the digital surveillance video camera dashboard within the security command center at the in-scope facilities to determine that digital surveillance video cameras recorded activities at facility entrances, the building perimeters, and other areas within the facilities.	No exceptions noted.
CC6.4.17	Digital surveillance video camera recordings are archived, allowing the capability for ad hoc investigations.	Inspected the digital surveillance recording configurations to determine that digital surveillance video camera recordings were archived, allowing the capability for ad hoc investigations.	No exceptions noted.
CC6.4.18	The data centers are monitored 24 hours per day with the use of motion-sensitive digital surveillance cameras, alarms, and motion detectors.	Observed the monitoring tools at the in-scope facilities to determine that the data centers were monitored 24 hours per day with the use of motion-sensitive digital surveillance cameras, alarms, and motion detectors.	No exceptions noted.
CC6.4.19	Security personnel monitor access to facility entrances and manage visitor access 24 hours per day.	Observed the security personnel at the security command center for the in-scope facilities to determine that security personnel monitored access to facility entrances and managed visitor access.	No exceptions noted.
		Inspected the most recent master shift schedule for security personnel across the in-scope facilities to determine that security personnel were staffed to monitor access to the facilities on a 24 hour per day basis during the period.	No exceptions noted.
CC6.4.20	Security personnel utilize an incident reporting system to document physical security incidents.	Inspected the listing of physical security incidents during the period within the incident reporting system to determine that security personnel utilized an incident reporting system to document physical security incidents during the period.	No exceptions noted.
CC6.4.21	The physical security hardware (e.g., monitoring servers, DVRs) is secured behind locked server racks and physical cages.	Observed the secured server racks and physical cages for the in-scope facilities to determine that the physical security hardware was secured behind locked server racks and physical cages.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.4.22	Physical access to the data center is documented and approved by the employee's manager prior to access being granted.	Inspected the physical access request approval for a sample of employees and contractors granted access during the period to determine that physical access to the data center was documented and approved by the employee's manager prior to access being granted for each employee and contractor sampled.	No exceptions noted.
CC6.4.23	Physical access to customer cages is documented and approved by the customer prior to access being granted.	Inspected the physical access request approval to customer cages for a sample of vendors and customers granted access during the period to determine that physical access to the customer cages was documented and approved by the customer prior to access being granted for each sample selected.	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 assets that are no longer needed.	Inspected the data retention and destruction policies and procedures to determine that retention periods and destruction procedures were defined for assets that were no longer needed.	No exceptions noted.
CC6.5.2	Physical assets are disposed of in accordance with data destruction policies.	Inspected the data destruction policies and procedures and the data disposal evidence for a sample of physical assets disposed during the period to determine that each physical asset sampled was disposed of in accordance with data destruction policies.	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	A firewall system is in place to filter unauthorized inbound network traffic from the Internet.	Inspected the firewall system ruleset for a sample of in-scope firewalls to determine that each firewall system sampled was configured to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
CC6.6.2	Network monitoring applications are utilized to monitor network devices and are configured to notify operations personnel via e-mail when predefined events occur on the network.	Inspected the network monitoring application configurations and example alerts generated during the period to determine that network monitoring applications were utilized to monitor network devices and were configured to notify operations personnel via e-mail when predefined events occurred on the network.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.6.3	Users communicate with network infrastructure devices via an SSH program to help ensure that communication sessions are encrypted using a cryptographic hash function.	Inquired of the Director of IT Compliance regarding logical access to network infrastructure to determine that users communicated with network infrastructure devices via an SSH program to ensure that communication sessions were encrypted using a cryptographic hash function.	No exceptions noted.
		Inspected the network infrastructure device configurations for a sample of network infrastructure devices to determine that communication sessions for each network infrastructure device sampled were encrypted using a cryptographic hash function.	No exceptions noted.
CC6.6.4	Encrypted VPNs are required for remote access to production and enforce two-factor authentication.	Inspected the VPN encryption and authentication configurations to determine that encrypted VPNs were utilized for remote access to production and enforced two-factor authentication.	No exceptions noted.
CC6.6.5	IT security personnel utilize a third-party utility to perform a vulnerability scan of the production servers on a monthly basis to identify threats and assess their potential impact to the production environment. Any security vulnerabilities that are identified are triaged by IT security personnel and monitored through resolution.	Inspected the vulnerability scan report and an example remediation ticket for a sample of months during the period to determine that IT personnel utilized a third-party utility to perform a vulnerability scan of the production servers to identify threats and assess their potential impact to the production environment and that security vulnerabilities that were identified were triaged by IT security personnel and monitored through resolution for each month sampled.	No exceptions noted.
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	Encrypted VPNs are required for remote access to production and enforce two-factor authentication.	Inspected the VPN encryption and authentication configurations to determine that encrypted VPNs were utilized for remote access to production and enforced two-factor authentication.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.7.2	Users communicate with network infrastructure devices via an SSH program to help ensure that communication sessions are encrypted using a cryptographic hash function.	Inquired of the Director of IT Compliance regarding logical access to network infrastructure to determine that users communicated with network infrastructure devices via an SSH program to ensure that communication sessions were encrypted using a cryptographic hash function.	No exceptions noted.
		Inspected the network infrastructure device configurations for a sample of network infrastructure devices to determine that communication sessions for each network infrastructure device sampled were encrypted using a cryptographic hash function.	No exceptions noted.
CC6.7.3	Procedures are in place that prohibit the transmission of sensitive information over the Internet or other public communications paths unless it is encrypted.	Inspected the information security policies and procedures to determine that procedures 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.
CC6.7.4	A mobile device and teleworking policy are in place to guide personnel in the proper use of mobile devices.	Inspected the mobile device and teleworking policy to determine that a mobile device and teleworking policy was in place to guide personnel in the proper use of mobile devices.	No exceptions noted.
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	A central antivirus server is configured with antivirus software to protect registered production Windows servers and workstations with the following configurations: • Scan for updates to antivirus definitions on a real-time basis • On-access scanning of executables and files	Inspected the enterprise antivirus software configurations and registered client list to determine that a central antivirus server was configured with antivirus software to protect registered production Windows servers and workstations with the following configurations: • Scan for updates to antivirus definitions on a real-time basis • On-access scanning of executables and files	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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	IT security personnel utilize a third-party utility to perform a vulnerability scan of the production servers on a monthly basis to identify threats and assess their potential impact to the production environment. Any security vulnerabilities that are identified are triaged by IT security personnel and monitored through resolution.	Inspected the vulnerability scan report and an example remediation ticket for a sample of months during the period to determine that IT personnel utilized a third-party utility to perform a vulnerability scan of the production servers to identify threats and assess their potential impact to the production environment and that security vulnerabilities that were identified were triaged by IT security personnel and monitored through resolution for each month sampled.	No exceptions noted.
CC7.1.2	The network domain is configured to log the following events: • Logon events • Object access • Policy changes • Process tracking • System events IT personnel review network domain event logs on an ad hoc basis.	Inquired of the Director of IT Compliance regarding the network domain log review process to determine that IT personnel reviewed network domain event logs on an ad hoc basis during the period.	No exceptions noted.
		Inspected the network domain logging configurations and an example event log generated during the period to determine that the network domain was configured to log the following events: • Logon events • Object access • Policy changes • Process tracking • System events	No exceptions noted.
CC7.1.3	The operating system is configured to log the following events: • Account logon events • Account management events • Logon events • Policy changes IT personnel review operating system event logs on an ad hoc basis.	Inquired of the Director of IT Compliance regarding the operating system log review process to determine that IT personnel reviewed operating system event logs on an ad hoc basis during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the operating system logging configurations for a sample of production servers and an example event log generated during the period to determine that each server sampled was configured to log the following events: • **Account logon events** • **Account management events** • **Logon events** • **Policy changes**	**No exceptions noted.**
CC7.1.4	Activity logs of certain physical movements within the facilities are monitored and maintained.	Inquired of the SVP of SecOps regarding physical access monitoring to determine that activity logs for movement within the facilities were logged and that personnel reviewed logs on an ad hoc basis in response to incidents and alarms.	No exceptions noted.
		Inspected example activity logs recorded during the period to determine that the following attributes for physical movements within the facilities were captured and maintained during the period: • Date / time • Event • Badge access card details • Device	No exceptions noted.
CC7.1.5	The firewall system is configured to log certain activity that includes, but is not limited to, the following: • Successful connections • Denied connections IT personnel review firewall system event logs on an ad hoc basis.	Inquired of the Director of IT Compliance regarding the firewall log review process to determine that IT personnel reviewed firewall system event logs on an ad hoc basis during the period.	No exceptions noted.
		Inspected the firewall system logging configurations for a sample of in-scope firewall systems to determine that each firewall system sampled was configured to log activity that included the following: • Successful connections • Denied connections	No exceptions noted.
CC7.1.6	The VPN system is configured to log certain activity that includes, but is not limited to, the following: • Failed login attempts • Successful login attempts IT personnel review VPN system event logs on an ad hoc basis.	Inquired of the Director of IT Compliance regarding the VPN log review process to determine that IT personnel reviewed VPN system event logs on an ad hoc basis during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the VPN system logging configurations and an example VPN system event log generated during the period to determine that the VPN system was configured to log activity that included the following: • Failed login attempts • Successful login attempts	No exceptions noted.
CC7.1.7	The centralized authentication system is configured to log events that include, but are not limited to, the following: • Successful logins • Failed logins • Administrator commands executed during an active session IT management reviews central authentication system event logs on an ad hoc basis.	Inquired of the Director of IT Compliance regarding the review of the centralized authentication system logs to determine that IT management reviewed central authentication system event logs on an ad hoc basis during the period.	No exceptions noted.
		Inspected the centralized authentication system logging configurations and example logs generated during the period to determine that the centralized authentication system was configured to log the following events: • Successful logins • Failed logins • Administrator commands executed during an active session	No exceptions noted.
CC7.1.8	Network monitoring applications are utilized to monitor network devices and are configured to notify operations personnel via e-mail when predefined events occur on the network.	Inspected the network monitoring application configurations and example alerts generated during the period to determine that network monitoring applications were utilized to monitor network devices and were configured to notify operations personnel via e-mail when predefined events occurred on the network.	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	Activity logs of certain physical movements within the facilities are monitored and maintained.	Inquired of the SVP of SecOps regarding physical access monitoring to determine that activity logs for movement within the facilities were logged and that personnel reviewed logs on an ad hoc basis in response to incidents and alarms.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected example activity logs recorded during the period to determine that the following attributes for physical movements within the facilities were captured and maintained during the period: • **Date / time** • **Event** • **Badge access card details** • **Device**	**No exceptions noted.**
CC7.2.2	Digital surveillance video cameras record activities at facility entrances, the building perimeters, and other areas within the facilities.	Observed the digital surveillance video camera dashboard within the security command center at the in-scope facilities to determine that digital surveillance video cameras recorded activities at facility entrances, the building perimeters, and other areas within the facilities.	No exceptions noted.
CC7.2.3	Digital surveillance video camera recordings are archived, allowing the capability for ad hoc investigations.	Inspected the digital surveillance recording configurations to determine that digital surveillance video camera recordings were archived, allowing the capability for ad hoc investigations.	No exceptions noted.
CC7.2.4	The data centers are monitored 24 hours per day with the use of motion-sensitive digital surveillance cameras, alarms, and motion detectors.	Observed the monitoring tools at the in-scope facilities to determine that the data centers were monitored 24 hours per day with the use of motion-sensitive digital surveillance cameras, alarms, and motion detectors.	No exceptions noted.
CC7.2.5	Security personnel monitor access to facility entrances and manage visitor access 24 hours per day.	Observed the security personnel at the security command center for the in-scope facilities to determine that security personnel monitored access to facility entrances and managed visitor access.	No exceptions noted.
		Inspected the most recent master shift schedule for security personnel across the in-scope facilities to determine that security personnel were staffed to monitor access to the facilities on a 24 hour per day basis during the period.	No exceptions noted.
CC7.2.6	Security personnel utilize an incident reporting system to document physical security incidents.	Inspected the listing of physical security incidents during the period within the incident reporting system to determine that security personnel utilized an incident reporting system to document physical security incidents during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.2.7	The data centers' temperature and humidity levels are systematically monitored. Operations personnel are notified via e-mail and text message when predefined minimum and maximum thresholds are exceeded.	Inquired of the SVP of SecOps regarding the monitoring of temperature and humidity levels at the in-scope facilities to determine that the data centers' temperature and humidity levels were systematically monitored and that operations personnel were notified via e-mail and text message when predefined minimum and maximum thresholds were exceeded.	No exceptions noted.
		Inspected the monitoring system configurations and example alerts generated during the period for the in-scope facilities to determine that the data centers' temperature and humidity levels were systematically monitored and that operations personnel were notified via e-mail and text message when predefined minimum and maximum thresholds were exceeded.	No exceptions noted.
CC7.2.8	Power levels are systematically monitored and configured to alert personnel when predefined minimum and maximum thresholds are exceeded.	Inspected the monitoring system configurations and an example alert generated during the period to determine that power levels were systematically monitored and configured to alert personnel when predefined minimum and maximum thresholds were exceeded.	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 escalation procedures for reporting security and availability incidents are provided to internal and external users to guide users in identifying and reporting failures, incidents, concerns, and other complaints.	Inspected the escalation procedures available on the company intranet and the customer-facing website to determine that documented escalation procedures for reporting security and availability incidents were provided to internal and external users to guide users in identifying and reporting failures, incidents, concerns, and other complaints.	No exceptions noted.
CC7.3.2	A dedicated NOC is staffed 24 hours per day to respond to customer inquiries, support issues, and incidents.	Inquired of the SVP of SecOps regarding customer support to determine that a dedicated NOC was staffed 24 hours per day to respond to customer inquiries, support issues, and incidents.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the NOC staffing schedule and the employee time report for a sample of weeks during the period to determine that the NOC was staffed 24 hours per day for each week sampled.	No exceptions noted.
CC7.3.3	IT personnel utilize an automated ticketing system to document security violations, responses, and resolution.	Inspected the ticketing system dashboard and the incident ticket for a sample of incidents that occurred during the period to determine that IT personnel utilized an automated ticketing system to document security violations, responses, and resolution for each incident sampled.	No exceptions noted.
CC7.3.4	Management meetings are held on a biweekly basis to discuss incidents and corrective measures to help ensure that incidents are resolved.	Inquired of the Director of IT Compliance regarding management meetings to determine that management meetings were held on a biweekly basis to discuss incidents and corrective measures to ensure that incidents were resolved.	No exceptions noted.
		Inspected the management meeting minutes for a sample of weeks during the period to determine that management meetings were held to discuss incidents and corrective measures for each week sampled.	No exceptions noted.
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 reporting security and availability incidents are provided to internal and external users to guide users in identifying and reporting failures, incidents, concerns, and other complaints.	Inspected the escalation procedures available on the company intranet and the customer-facing website to determine that documented escalation procedures for reporting security and availability incidents were provided to internal and external users to guide users in identifying and reporting failures, incidents, concerns, and other complaints.	No exceptions noted.
CC7.4.2	IT personnel utilize an automated ticketing system to document security violations, responses, and resolution.	Inspected the ticketing system dashboard and the incident ticket for a sample of incidents that occurred during the period to determine that IT personnel utilized an automated ticketing system to document security violations, responses, and resolution for each incident sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.			
CC7.5.1	Documented escalation procedures for reporting security and availability incidents are provided to internal and external users to guide users in identifying and reporting failures, incidents, concerns, and other complaints.	Inspected the escalation procedures available on the company intranet and the customer-facing website to determine that documented escalation procedures for reporting security and availability incidents were provided to internal and external users to guide users in identifying and reporting failures, incidents, concerns, and other complaints.	No exceptions noted.
CC7.5.2	IT personnel utilize an automated ticketing system to document security violations, responses, and resolution.	Inspected the ticketing system dashboard and the incident ticket for a sample of incidents that occurred during the period to determine that IT personnel utilized an automated ticketing system to document security violations, responses, and resolution for each incident sampled.	No exceptions noted.
CC7.5.3	Management meetings are held on a biweekly basis to discuss incidents and corrective measures to help ensure that incidents are resolved.	Inquired of the Director of IT Compliance regarding management meetings to determine that management meetings were held on a biweekly basis to discuss incidents and corrective measures to ensure that incidents were resolved.	No exceptions noted.
		Inspected the management meeting minutes for a sample of weeks during the period to determine that management meetings were held to discuss incidents and corrective measures for each week sampled.	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	Documented policies and procedures are in place to address the following: • Defined categories of changes • Change initiation, testing, and approval prior to implementation in production • Roles and responsibilities of process owners • Emergency change process	Inspected the change management policies and procedures to determine that documented policies and procedures were in place to address the following: • Defined categories of changes • Change initiation, testing, and approval prior to implementation in production • Roles and responsibilities of process owners • Emergency change process	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC8.1.2	Change management meetings are held on a weekly basis to discuss and communicate the ongoing and upcoming projects that affect the system.	Inspected the recurring calendar meeting invitation, agenda, and minutes for a sample of weeks during the period to determine that change management meetings were held to discuss and communicate the ongoing and upcoming projects that affected the system for each week sampled.	No exceptions noted.
CC8.1.3	Automated ticketing systems are utilized to log and track in-scope system infrastructure change information, impacted system resources, and management approvals.	Inspected the ticketing system for a sample of infrastructure changes implemented during the period to determine that automated ticketing systems were utilized to log and track the information, impacted system resources, and management approvals for each change sampled.	No exceptions noted.
CC8.1.4	Infrastructure changes are authorized, tested where applicable, and approved prior to implementation.	Inquired of the Director of IT Compliance regarding infrastructure changes to determine that infrastructure changes were authorized, tested where applicable, and approved prior to implementation.	No exceptions noted.
		Inspected the change management documentation for a sample of infrastructure changes implemented during the period to determine that each change sampled was authorized, tested where applicable, and approved.	No exceptions noted.
CC8.1.5	The ability to implement infrastructure changes is restricted to user accounts accessible by authorized personnel.	Inspected the listing of user accounts with the ability to implement infrastructure changes with the assistance of the Manager of IT Compliance to determine that the ability to implement infrastructure changes was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
Risk Mitigation			
CC9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
CC9.1.1	Documented procedures are in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process.	Inspected the risk assessment procedures to determine that documented procedures were in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC9.1.2	A risk assessment is performed on an annual basis that includes an evaluation of risk mitigation control activities for 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 documentation to determine that a risk assessment was performed that included an evaluation of risk mitigation control activities for risks arising from potential business disruptions, and that identified risks were rated using a risk evaluation process and were formally documented, with mitigation strategies, for management review during the period.	No exceptions noted.
CC9.1.3	Business resiliency plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.	Inspected the business resiliency plans to determine that business resiliency plans were in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.	No exceptions noted.
CC9.2 The entity assesses and manages risks associated with vendors and business partners.			
CC9.2.1	Documented vendor management policies are in place to address the following: • Access control for a vendor or business partner • Due diligence process prior to accepting new vendors or business partners • Monitoring process to review vendor and business partner compliance on a periodic basis • Termination of contract	Inspected the vendor supplier security policies to determine that documented vendor management policies were in place to address the following: • Access control for a vendor or business partner • Due diligence process prior to accepting new vendors or business partners • Monitoring process to review vendor and business partner compliance on a periodic basis • Termination of contract	No exceptions noted.
CC9.2.2	The threats arising from the use of vendors and third parties are considered by senior management as part of the annual risk assessment and IT security planning process.	Inspected the most recent risk assessment documentation to determine that threats arising from the use of vendors and third parties were considered by senior management as part of the risk assessment and IT security planning process during the period.	No exceptions noted.
CC9.2.3	Management performs due diligence prior to onboarding a vendor or business partner to help ensure third parties are in compliance with the organization's security and availability commitments.	Inspected the vendor risk assessment for a sample of vendors onboarded during the period to determine that management performed due diligence to ensure third parties were in compliance with the organization's security and availability commitments prior to onboarding for each vendor sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC9.2.4	Management reviews vendor audit reports on an annual basis to help ensure that vendors or business partners are in compliance with the organization's security and availability commitments.	Inspected the vendor review for a sample of in-scope vendors to determine that management reviewed vendor audit reports to ensure that each vendor sampled was in compliance with the organization's security and availability commitments during the period.	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	Network monitoring applications are utilized to monitor network devices and are configured to notify operations personnel via e-mail when predefined events occur on the network.	Inspected the network monitoring application configurations and example alerts generated during the period to determine that network monitoring applications were utilized to monitor network devices and were configured to notify operations personnel via e-mail when predefined events occurred on the network.	No exceptions noted.
A1.1.2	The data centers' temperature and humidity levels are systematically monitored. Operations personnel are notified via e-mail and text message when predefined minimum and maximum thresholds are exceeded.	Inquired of the SVP of SecOps regarding the monitoring of temperature and humidity levels at the in-scope facilities to determine that the data centers' temperature and humidity levels were systematically monitored and that operations personnel were notified via e-mail and text message when predefined minimum and maximum thresholds were exceeded.	No exceptions noted.
		Inspected the monitoring system configurations and example alerts generated during the period for the in-scope facilities to determine that the data centers' temperature and humidity levels were systematically monitored and that operations personnel were notified via e-mail and text message when predefined minimum and maximum thresholds were exceeded.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.1.3	A dedicated NOC is staffed 24 hours per day to respond to customer inquiries, support issues, and incidents.	Inquired of the SVP of SecOps regarding customer support to determine that a dedicated NOC was staffed 24 hours per day to respond to customer inquiries, support issues, and incidents.	No exceptions noted.
		Inspected the NOC staffing schedule and the employee time report for a sample of weeks during the period to determine that the NOC was staffed 24 hours per day for each week sampled.	No exceptions noted.
A1.1.4	Management meetings are held on a biweekly basis to discuss incidents and corrective measures to help ensure that incidents are resolved.	Inquired of the Director of IT Compliance regarding management meetings to determine that management meetings were held on a biweekly basis to discuss incidents and corrective measures to ensure that incidents were resolved.	No exceptions noted.
		Inspected the management meeting minutes for a sample of weeks during the period to determine that management meetings were held to discuss incidents and corrective measures for each week sampled.	No exceptions noted.
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	The data center facilities are equipped with the following environmental protection equipment: • Fire detection and suppression equipment • UPS systems • Generators • Air conditioning units to protect against fire and smoke damage, keep infrastructure at optimal temperatures, and provide uninterrupted power to maintain availability commitments	Observed the environmental protection equipment within the in-scope facilities to determine that the data center facilities were equipped with the following environmental protection equipment: • Fire detection and suppression equipment • UPS systems • Generators • Air conditioning units to protect against fire and smoke damage, keep infrastructure at optimal temperatures, and provide uninterrupted power to maintain availability commitments	No exceptions noted.
A1.2.2	The business process director obtains inspection reports as evidence that the fire suppression systems undergo maintenance inspections on a quarterly basis.	Inspected the fire suppression system inspection report for a sample of quarters during the period for the in-scope facilities to determine that the fire suppression systems underwent maintenance inspections for each quarter sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.2.3	The business process director obtains inspection reports as evidence that the fire alarm systems undergo maintenance inspections on a quarterly basis.	Inspected the fire alarm system inspection report for a sample of quarters during the period for the in-scope facilities to determine that the fire alarm systems underwent maintenance inspections for each quarter sampled.	No exceptions noted.
A1.2.4	The business process director obtains inspection tags as evidence that the hand-held fire extinguishers undergo maintenance inspections on an annual basis.	Observed the inspection tag for a sample of hand-held fire extinguishers at the in-scope facilities to determine that each hand-held fire extinguisher sampled underwent maintenance inspections during the period.	No exceptions noted.
A1.2.5	The business process director obtains inspection reports as evidence that the air conditioning systems undergo maintenance inspection on a quarterly basis.	Inspected the air conditioning system inspection report for a sample of quarters during the period for the in-scope facilities to determine that the air conditioning systems underwent maintenance inspection for each quarter sampled.	No exceptions noted.
A1.2.6	Internal personnel inspect and maintain the air conditioning systems on at least a quarterly basis to help ensure that they are functioning properly.	Inspected the air conditioning system inspection report for a sample of quarters during the period for the in-scope facilities to determine that internal personnel inspected and maintained the air conditioning systems for each quarter sampled.	No exceptions noted.
A1.2.7	The business process director obtains inspection reports as evidence that the generators undergo maintenance inspections on a quarterly basis.	Inspected the generator inspection report for a sample of quarters during the period for the in-scope facilities to determine that the generators underwent maintenance inspections for each quarter sampled.	No exceptions noted.
A1.2.8	Internal personnel perform preventative maintenance procedures on the generators on a quarterly basis.	Inspected the generator inspection report for a sample of quarters during the period for the in-scope facilities to determine that internal personnel performed preventative maintenance procedures on the generators for each quarter sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.2.9	UPS systems undergo documented maintenance inspections on a semi-annual basis.	Inspected the most recent UPS system inspection report for the in-scope facilities to determine that the UPS systems underwent documented maintenance inspections during the six months preceding the end of the period for the following in-scope data center facilities: • LAS 2 • LAS 4 • LAS 5 • LAS 7 • LAS 8 • LAS 9 • LAS 10 • LAS 11 • LAS 12 • LAS 15 • RNO 1 • GRR 1 • ATL 1	**No exceptions noted.**
		Inspected the data center operations maintenance schedule and the go-live date of the RNO 2 data center facility with the assistance of the VP of Data Center Operations and determined that there were no UPS maintenance inspections required for RNO 2 during the period since the systems were newly installed; therefore, no testing of operating effectiveness was performed.	
A1.2.10	A dedicated NOC is staffed 24 hours per day to respond to customer inquiries, support issues, and incidents.	Inquired of the SVP of SecOps regarding customer support to determine that a dedicated NOC was staffed 24 hours per day to respond to customer inquiries, support issues, and incidents.	No exceptions noted.
		Inspected the NOC staffing schedule and the employee time report for a sample of weeks during the period to determine that the NOC was staffed 24 hours per day for each week sampled.	No exceptions noted.
A1.2.11	Business resiliency plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.	Inspected the business resiliency plans to determine that business resiliency plans were in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.	No exceptions noted.
A1.2.12	Contingency planning procedures are in place to guide personnel in contingency planning activities.	Inspected the contingency planning procedures to determine that contingency planning procedures were in place to guide personnel in contingency planning activities.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.3 The entity tests recovery plan procedures supporting system recovery to meet its objectives.			
A1.3.1	Disaster recovery plans are tested on at least an annual basis.	Inspected the results of the most recent disaster recovery test to determine that disaster recovery plans were tested during the period.	No exceptions noted.

SECTION 5

OTHER INFORMATION PROVIDED BY SWITCH

DISASTER AVOIDANCE

Nevada provides an ideal setting for data center facilities as the area is considered a "safe-zone" from natural disasters. Nevada also has a highly sophisticated power grid and is a prime gateway for data flow from the West Coast to the East Coast.

NEVADA POWER GRID

Why Nevada for Power?

Nevada's alternative energy capacity is unique in the United States with a rare and rich blend of solar, wind and geothermal resources. These resources and capacities set Nevada apart as an ideal state for sustainable energy. Specifically, Nevada offers the nation's leading solar radiance and temperate windows, perfect for photovoltaic and solar concentration solutions.[1] Additionally, Nevada's wind capacity alone has been estimated as capable of supporting 60 percent of the state's needs.[2] Lastly, Nevada's geothermal solutions are among the oldest in the nation and growing. As the Las Vegas Sun has reported, "Nevada is poised to overtake California as the American geothermal energy leader. All of this is undergirded with natural gas lines that run through Las Vegas, Carson City, and Reno to supply the major population centers. In short, Nevada is perfectly poised to provide clean, affordable, and renewable energy.

Nevada's electrical grid is also robust and resilient. Nevada's climate, predictable and moderate weather patterns, and lack of natural disasters make Nevada ideal for electrical distribution and transmission and telecommunications networks. While other states are constantly required to repair, refurbish, and rebuild electrical systems to compete with corrosion and severe weather, Nevada's grids enjoy the mild seasonality and humidity of Nevada's temperate deserts.

Energy sustainability and self-sufficiency are becoming increasingly important for mission critical services. As the world begins to stir out of the global recession, industrialized nations' need for oil to fuel their factories and transportation and economies will continue to increase. The United States is not yet self-sufficient when it comes to oil. Month after month, the United States still imports about two-thirds of the oil consumed and 70 percent of that use is for transportation fuel. Nevada's unique renewable energy capabilities offer environmental responsibility and economic stability in the face of national dependence on fluctuating oil prices.

Where Does Switch Power Come from in Nevada?

Switch is committed to supporting its operations with 100 percent renewable and clean power, including power from Switch Station 1 and Switch Station 2, to provide 180 megawatts of photovoltaic generation. Securing 100 percent of Switch's energy from renewable sources is a central part of Switch's strategy and commitment to being planet friendly.

[1] See data provided by NREL, available at:
http://interestingenergyfacts.blogspot.com/2008/04/us-solar-energy-map.html

[2] See data provided by NREL, available at:
http://apps2.eere.energy.gov/wind/windexchange/wind_resource_maps.asp?stateab=nv

SWITCH, LTD.

INDEPENDENT SERVICE AUDITOR'S SOC 3 REPORT

FOR THE

SWITCH COLOCATION SERVICES

FOR THE PERIOD OF OCTOBER 1, 2022, TO SEPTEMBER 30, 2023

Attestation and Compliance Services

schellman

INDEPENDENT SERVICE AUDITOR'S REPORT

To Switch, Ltd.:

Scope

We have examined Switch, Ltd.'s ("Switch") accompanying assertion titled "Assertion of Switch Service Organization Management" ("assertion") that the controls within Switch's Colocation Services system ("system") were effective throughout the period October 1, 2022, to September 30, 2023, to provide reasonable assurance that Switch'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).*

Service Organization's Responsibilities

Switch 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 Switch's service commitments and system requirements were achieved. Switch has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Switch is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

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

Our examination included:

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

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

Inherent Limitations

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

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

Opinion

In our opinion, management's assertion that the controls within Switch's Colocation Services system were effective throughout the period October 1, 2022, through September 30, 2023, to provide reasonable assurance that Switch's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Schellman & Company, LLC

Tampa, Florida
November 8, 2023

ASSERTION OF SWITCH SERVICE ORGANIZATION MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within Switch, Ltd.'s ("Switch") Colocation Services system ("system") throughout the period October 1, 2022, to September 30, 2023, to provide reasonable assurance that Switch's service commitments and system requirements relevant to security and availability were achieved. Our description of the boundaries of the system is presented below and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period October 1, 2022, to September 30, 2023, to provide reasonable assurance that Switch'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)*. Switch's objectives for the system in applying the applying the applicable trust services criteria are embodied in its service commitments and systems requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented below.

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

We assert that the controls within the system were effective throughout the period October 1, 2022, to September 30, 2023, to provide reasonable assurance that Switch's service commitments and systems requirements were achieved based on the applicable trust services criteria.

DESCRIPTION OF THE BOUNDARIES OF THE SWITCH COLOCATION SERVICES SYSTEM

Company Background

Switch is a technology infrastructure ecosystem corporation whose core business is the design, construction, and operation of data centers. Founded in 2000 and headquartered in Las Vegas, Nevada, Switch is built on the intelligent and sustainable growth of the Internet. The Founder and CEO, Rob Roy, has developed more than 700 issued and pending patent claims covering data center designs that manifested into Switch data centers and technology solution ecosystems. Since the opening of their first colocation facility, Switch has delivered 100% uptime across their facilities. At Switch, every team member is driven to produce real results for their clients – technologically and financially. Switch data center ecosystems empower their clients with numerous options for innovation, economies of scale, risk mitigation, sustainability, and investment protection.

Company Profile

Switch's advanced data centers are the center of their platform and provide power densities that exceed industry averages with efficient cooling, while being powered by 100% renewable energy. Two of the Switch data centers are the only carrier-neutral colocation facilities in the world to be certified Tier IV Design, Tier IV Facility, and Tier IV Gold in Operational Excellence. While these certifications have been the highest classifications available in the industry, Switch is building their current facilities to their proprietary Tier 5 Platinum standards, which exceed Tier IV standards. Switch's platform has powerful network effects and nurtures a technology ecosystem that benefits its participants. Switch continues to further enhance these benefits as they innovate and expand their platform ecosystem. Switch currently has over 1,000 customers, including technology and digital media companies, cloud, and managed service providers, financial institutions, and telecommunications providers.

The growing nexus between Internet connectivity, Internet-based services, data and analytics, and the advancement of computational processing power is rapidly expanding the amount of data that enterprises can access and manage. At the same time, the Internet of Everything is exponentially expanding the available data sources, as utility grids, automobiles, aircraft, home appliances, wearable devices, and numerous other sources are all connecting to the Internet. The compute capacity necessary to manage and analyze this data is also advancing and demanding increasing amounts of power to operate. Switch believes that traditional technology infrastructure is not capable of supporting the growing wave of mission critical data and increasingly powerful IT equipment.

Switch presently owns and operates four primary campus locations, called Primes, which encompass fourteen colocation facilities with an aggregate of over 5.3 million gross square feet (GSF) of space. These facilities have approximately 470 megawatts (MW) of power available to them. Primes consist of The Core Campus in Las Vegas, Nevada; The Citadel Campus near Reno, Nevada; The Pyramid Campus in Grand Rapids, Michigan; and The Keep Campus in Atlanta, Georgia. Primes are strategically located in geographies that combine a low risk of natural disaster, favorable tax policies for customers deploying computing infrastructure, and low latency connectivity to major metropolitan markets, such as Los Angeles, San Francisco, Silicon Valley, Chicago, New York, Northern Virginia, and Miami. As a result, customers in these metropolitan markets can access Switch's colocation facilities while reducing exposure to higher taxes, higher cost of power, and higher risk of natural disaster that might be prevalent in other markets. Switch can also use their Switch Modular Optimized Design (MOD) technology to build single-user facilities and are actively pursuing opportunities to deploy this technology in a build-to-suit offering for their enterprise customers.

As additional locations and sectors within the four existing Prime campus locations are opened for Colocation Services, the same / similar controls tested within this report are implemented / in place.

Description of Services Provided

Physical Security

Exterior Barriers

From well-defined perimeters consisting of signage, blast walls, and gates, to clear avenues of approach and backup perimeter barriers, the first layer of physical security is extensive. Exterior walls are constructed of either steel reinforced poured concrete or masonry reinforced beyond building code requirements. Entry points are kept to a minimum and each exterior door is reinforced, alarmed, access-controlled, and viewed by two dedicated fixed cameras.

Interior Barriers and Customer Compartmentalization

Exterior doors lead into specially engineered mantraps built over fire corridor wall construction. The mantraps are sheeted with steel and seams are strapped by aluminum. Access points off the mantrap require additional multi-factor biometric authentication of the card holder and are controlled via a 24 hour per day security officer and mantrap relay logic. Each mantrap includes fixed cameras viewing each door.

Each customer space, whether it is a cage, cabinet, or suite, is individually locked, protected, and monitored. Additional security safeguards, such as mantraps, intrusion sensors, and surveillance cameras, can be added to these spaces at the customer's request.

Positive Access Control

Positive Access Control is the application of a two-fold access principle stemming from the questions, "Who are you? And why should we let you in?" When first granted access to the facility, a multi-step process is in place to determine identity and verify need for access. In addition to the metal walls, turnstiles, cameras, intercoms, and biometric readers, Switch's access control takes on further hardening by the Positive Access Control procedures deployed at the facilities. Positive Access Control requires that a proprietary 24 hours per day officer staffed security command center (SECOM) verifies that the person standing in the mantrap matches a file photo. After confirmation, the officer activates the second proximity and biometric reader for use.

The access process is further continued with periodic access audits performed each shift by the shift supervisor. Customer audits are conducted monthly by the campus security manager. A complete audit of personnel with access to the facilities is conducted by the Security Director on a semi-annual basis.

Surveillance

Surveillance equipment for the facilities follows an elite standard set by a board-certified security professional. Fixed cameras are high-resolution color (520 lines) or digital high definition (HD) with automatic low light switching, capable of viewing up to 0.1 lux. Pan / tilt / zoom (PTZ) cameras are used on the exterior and areas of sensitivity. Video is digitally recorded at common interchange format (CIF) resolution at 15 images per second (IPS) upon motion at 4CIF 30 IPS upon operator command or at select zones requiring enhanced video. Video is retained for 100 +/- 10 days.

Switch deploys active surveillance with on-staff officers operating the camera system 24 hours per day. Camera operators use the Identify, Observe and Understand (IOU) methodology. The IOU methodology includes constant monitoring, use of cameras for detection, and a usable video product for investigations.

Sensors

Detectors are used around the property and provide early warning for perimeter and sensitive area intrusion. Sensor types include infrared motion, ultrasonic motion, photoelectric motion, electromechanical, internal lock, and seismic. These sensors are installed based on the environment or protection needs.

Security Team

Switch has a proprietary SECOM fully staffed 24 hours per day. Security staff members are hired with military and law enforcement security experience and must complete an extensive training period, which includes security system instruction, procedure and policy instruction, and non-lethal weapon training. The Security Academy was

developed in accordance with the current American Society for Industrial Security (ASIS) International Guideline on Private Security Officer Selection and Training (ASIS GDL PSO-2010) and the 90-day field training officer (FTO) program. A security supervisor oversees each shift and reports to the campus security manager. Security supervisors are required to attend a Security Management course, and officers in management positions are required to be active members of ASIS International.

Please refer to the following link for related pictures and detailed information: http://www.switch.com.

Infrastructure Operations (Environmental Security)

Switch employs the latest advanced environmental controls to protect the systems of its customers as well as operating with energy efficiency. These systems are managed and monitored by the Data Center Operations (DCO) and Energy Management Systems (EMS) teams.

Fire Protection

Fire protection includes fire, smoke, and heat detection monitored 24 hours per day. Sensors are located throughout the data centers and provide alerts to physical security personnel and a third-party monitoring company for response. Data center areas are protected by aspirating smoke detectors, which are programmed to identify smoke in the incipit stage.

The data centers are equipped with dual-interlock pre-action dry pipe sprinklers. Specifically, these dual-interlock pre-action sprinklers require both a smoke detection event and the activation of sprinklers to release water into the pipes. This allows for quick response to a fire with a lower risk of water damage in the case of a smaller fire or false alarm.

Heating, Ventilation, and Cooling (HVAC)

Switch utilizes advanced, patented techniques starting with a custom-designed thermal separate compartment in facility or (t-scif) air-flow system. This airflow system pulls the warm air away from customer systems into a separate compartment. The warm air is taken out of the core SUPERNAP facility designed for 74 high-grade Switch-designed and patented TSC-600 and TSC-1000 HVAC units which are physically adjacent to the data center, each containing six types of air conditioning systems. Within the data centers, areas where warm or hot air travels are marked in red.

Please refer to the following link for related pictures and detailed information: http://www.switch.com.

Power Management

Switch utilizes multiple in-bound connections from electricity providers. Tri-redundant power systems, which balance dual in-bound power connections across three sources of power, optimize the power utilization. Power is currently provided in redundancy through the use of uninterruptable power supply (UPS) devices which are fed by generators across the campuses. Power distribution units are managed and secured to prevent tampering. Power cabling within the data center is color-coded for quick and succinct identification of circuits and to assist with troubleshooting.

Please refer to the following link for related pictures and detailed information: http://www.switch.com.

Support for Colocation Services

Switch maintains dedicated support for its customers 24 hours per day via the Network Operations Center (NOC). NOC and engineering staff are available to assist with network troubleshooting and provide "hands-on" services to support customers.

NOC representatives follow defined procedures to facilitate confirmation of identification, customer communication of unexpected events that may impact their systems, customer authorization (only authorized customer representatives can open a service request), and functional escalation for customer service requests and incidents. NOC representatives monitor customer inquiries, support issues, and incidents on a real-time basis. Issues are documented in the Living Data Center (LDC) ticketing system and tracked to resolution.

The ticketing system / customer relationship management (CRM) system contains a complete purchased product hierarchy, installed equipment, and the physical and logical infrastructure layouts of individual customer solutions. The complete history of customer service requests and incidents are recorded in the ticketing system. Customer-specific information is handled confidentially through permission-access levels in the ticketing system and access to customer infrastructures. Documented procedures are in place for the monitoring of customer support operations. Furthermore, volume analysis, response times, and procedural adherence are monitored to help ensure customer obligations are met.

Network Management and Monitoring (Logical Security)

Since Switch has no logical access to any customer's equipment or data, each customer is responsible for its own network security. Switch manages the network connectivity to the Internet via its multiple providers. Switch's core routers are managed by the network engineering team and monitored by the NOC 24 hours per day. Routers are configured for high availability in active-active mode such that if one fails or connectivity is lost, network traffic is diverted accordingly.

System Boundaries

The scope of this report is limited to the Colocation Services for the following facilities:

- Las Vegas, Nevada
  - Las Vegas 2 (LAS 2)
  - Las Vegas 4 (LAS 4)
  - Las Vegas 5 (LAS 5)
  - Las Vegas 7 (LAS 7)
  - Las Vegas 8 (LAS 8)
  - Las Vegas 9 (LAS 9)
  - Las Vegas 10 (LAS 10)
  - Las Vegas 11 (LAS 11)
  - Las Vegas 12 (LAS 12)
  - Las Vegas 15 (LAS 15)
- Reno, Nevada
  - Reno 1 (RNO 1)
  - Reno 2 (RNO 2)
- Grand Rapids, Michigan
  - Grand Rapids 1 (GRR 1)
- Atlanta, Georgia.
  - Atlanta 1 (ATL 1)

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.

Significant Changes During the Period

The RNO 2 data center facility was operational as of May 1, 2023. The test of controls at the facility only apply to the facility's dates of operation during the specified reporting period of May 1, 2023, to September 30, 2023, for the RNO 2 data center facility.

Principal Service Commitments and System Requirements

Switch designs business processes and procedures to meet its objectives for its Colocation Services. Those objectives are based on the service commitments that Switch makes to user entities, the laws and regulations that govern the provisioning of Colocation Services, and the financial, operational, and compliance requirements that Switch has established for the services.

Principal Service Commitments

Security and availability commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Switch makes the following principal service commitments to their customers:

- Make available Switch's colocation and/or other services to customers for the service term
- Establish, implement, and maintain commercially reasonable industry standards designed to protect the customers' equipment
- Provide services to customers in accordance with the service level goals
- Make available Switch's colocation space 24 hours per day, 7 days a week
- Offer service to customers regarding network availability, network latency, packet delivery, and power delivery
- Provide 99.99% availability of the Switch network in any calendar month
- Provide 100% power availability
- Availability of HVAC capacity to maintain temperatures in the area around the colocation space

System Requirements

Switch establishes operational requirements that support the achievement of the principal service commitments, relevant laws and regulations, and other system requirements. These requirements include account and password management processes, vulnerability assessment and remediation processes, and employee background screening and security awareness training. Additional requirements are the necessary system change management procedures to support the requisite authorization, documentation, testing, and approval of system changes.

System requirements are communicated in Switch's policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired, trained, and managed. Switch also has procedures in place to review documentation from third-party providers to ensure that they are in compliance with security and availability policies. Commitments and requirements of Switch are documented in customer contracts and are updated and signed upon any changes in the practices.

In accordance with Switch'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.

Infrastructure and Software

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

Primary Infrastructure			
Production System	**Business Function Description**	**Operating System Platform**	**Physical Location**
The Living Data Center (LDC) Application	Overall environmental conditions monitoring as well as ticketing system capability to track incidents and resolutions.	Linux	Las Vegas, Nevada Reno, Nevada Grand Rapids, Michigan Atlanta, Georgia
Microsoft Active Directory Domain	Network domain supporting internal systems applicable to the Colocation Services.	Windows	
Cisco Border and Private Routers	Network devices in place to direct traffic and filter unauthorized inbound network traffic from the Internet.	Cisco Internetwork Operating System (IOS)	
Honeywell Badge Access System	Physical access control supporting the Colocation Services at the Las Vegas, Reno, and Grand Rapids facilities that was decommissioned during November 2022. The in-scope facilities using Honeywell transitioned to C-Cure prior to the end of November 2022.	Windows	
C-Cure Badge Access System	Physical access control supporting the Colocation Services at the Las Vegas, Reno, Grand Rapids, and Atlanta facilities.		

In addition, Switch utilizes CrowdStrike antivirus software for antivirus protection for the Windows production servers and workstations. Furthermore, Switch utilizes Milestone Video Management System (VMS) for managing the security cameras for the interior and exterior of the data centers.

People

Switch utilizes specific functional areas of operations that support the scope of this review that include, but are not limited to, the following:

- Executive Management – responsible for overseeing company-wide activities, establishing, and accomplishing goals, and overseeing objectives.
- Security Operations (SecOps) department – responsible for monitoring and protecting the facility from unauthorized access, damage, and interference.
- Network Operations (NetOps) department – responsible for implementation of product development and optimization, client implementation, and technical operations.
- Data Center Operations (DCO) – responsible for monitoring and maintaining critical infrastructure including electrical and cooling infrastructure. Also responsible for preparing customer environment (cage, cabinet) and performing everyday maintenance of the facility.
- Energy Management Systems (EMS) department – responsible for monitoring and maintaining critical infrastructure including power equipment and infrastructure.
- Network Engineering department – responsible for managing network architecture.

- Facilities Services department – responsible for providing user entities with assistance before and after the initial sale by providing information, guidance, and continued support.
- Human Resources (HR) department – responsible for HR policies, practices, and processes with a focus on key HR department delivery areas (e.g., talent acquisitions, employee retention, compensation, employee benefits, performance management, employee relations, development, and employee-related incidents and investigations).
- Legal department – responsible for legal and regulatory issues involving corporate risk and corporate compliance.

Procedures

Access, Authentication, and Authorization

In order to gain access to the firewalls and routers, a user must authenticate with a user account and password via a secure shell (SSH) program to help ensure that the sessions are encrypted. The routers may only be managed from an internal network as SSH is not running on the public portion of the routers. SSH sessions are programmed to terminate a session after a predefined period of inactivity.

The network engineering team manages the security administration of the firewalls and routers and is required to authenticate through a terminal access controller access-control system plus (TACACS+) server which allows for individualized user account access, administration, and logging. These unique user accounts are defined by the TACACS+ server and are configured to authenticate using the corporate network domain.

The network domain is configured to enforce password requirements that include minimum length, expiration intervals, complexity, minimum history, and invalid account lockout threshold. Additionally, the operating system and badge access system are also configured to inherit credentials from the corporate network domain. Encrypted VPNs are required for remote access to production and enforce two-factor authentication.

Predefined access groups are employed within the network domain, operating system, badge access system, VPN system, and centralized authentication system to limit access based on job responsibilities. Additionally, administrator access to the aforementioned systems is restricted to only those personnel responsible for those activities via user account permissions and group assignments. Management reviews employee access privileges on a semi-annual basis.

IT management has configured the network domain, operating system, badge access system, VPN system, firewalls, and centralized authentication system to log access related events. IT management reviews these logs on an ad hoc basis to determine if any suspicious or unauthorized activity has occurred.

Access Requests and Access Revocation

Upon hire, an employee's production system access is requested, communicated, and approved by the employee's manager. The system access request details the specific production systems and required levels of access privileges. When an employee ends their employment, a termination checklist is completed to document the offboarding procedures performed and production system access is revoked.

Physical Asset Disposal

Documented data retention and destruction policies and procedures are in place to define retention periods and destruction procedures for assets that are no longer needed. When technology assets reach the end of their useful life, they are sent to the local IT team for disposal. IT personnel securely erase storage media in accordance with data destruction policies and procedures. Depending on the level of sensitivity of data contained on equipment being destroyed, physical destruction may be required. Destruction of computer equipment is performed off-site by a third-party vendor which issues certificates of destruction to confirm the destruction.

Physical Security

Switch has implemented various physical security protocols to protect the business premises and information systems from unauthorized access. A badge access system is in place 24 hours per day to control access to the office. Predefined access groups are utilized to provide access depending on the individual's role and responsibilities. Physical access to the data center is documented and approved by the employee's manager prior to access being granted, while physical access to customer cages is documented and approved by the customer prior to access being granted. Badge access attempts are logged by the system and are traceable to specific badge access cards. Management reviews employee and customer access privileges on a semi-annual basis. The ability to administer the badge access system is restricted to authorized security management personnel. If an individual who has physical access to the Switch facilities is terminated, security management personnel revoke the badge access privileges within 24 hours as a component of the termination process.

The building perimeters for the facilities include fences, walls, and entrance gates controlled by guards or card access. In addition, surveillance cameras are utilized by security personnel to monitor the main entrance to the facilities in order to identify visitors and contractors prior to granting access to the facilities. Visitors must present photo identification before being granted access to the facilities. Personnel at the facilities are distinguished as being an employee, customer, or contractor with a functioning color-coded badge access card or a visitor with a non-functioning visitor badge. Prior to being granted access to the secure interior of the data centers, personnel and authorized customers must enter a mantrap where they must scan the badge access card and provide biometric credentials. Personnel and authorized visitors are required to provide badge access cards and biometric identification for both entry and exit of interior doors. Visitors without badge access cards are required to be escorted by authorized employees while within the facilities.

Switch maintains and monitors activity logs of certain physical movements within the facilities on an as needed basis. Physical movements captured and monitored include date / time, event, badge access card details, and device. Digital surveillance cameras are in place to monitor the facility entrances, the building perimeters, and other areas within the facilities. Video surveillance captured by the camera system is archived allowing the capability for review as needed. The facilities are monitored 24 hours per day by security personnel with the use of motion-sensitive digital surveillance cameras, alarms, and motion detectors. The physical security hardware (e.g., monitoring servers, DVRs) is secured behind locked server racks and physical cages. An incident reporting system is utilized by security personnel to document any physical security incidents.

Environmental Security

Switch has implemented various environmental security protocols to protect the business premises and information systems from potential environmental issues. The Switch facilities are protected by fire detection and suppression equipment that includes fire alarms, dry-pipe water sprinklers, fire and smoke detectors, hand-held fire extinguishers, and smoke and heat sensors. On a quarterly basis, the fire detection and suppression equipment undergo an inspection from a third-party specialist to help ensure that the equipment is in proper working order. Hand-held fire extinguishers undergo maintenance inspections on an annual basis.

Management utilizes an environmental monitoring tool which is configured to systematically monitor the humidity and temperature levels within the Switch data centers. The system is configured to automatically send e-mail notifications to operations personnel when predefined thresholds are exceeded. An inspection matrix guides the frequency of inspection for critical infrastructure including power and cooling systems.

The data centers are designed to optimize cool air flow and utilize redundant air conditioning units to keep infrastructure equipment at optimal temperatures. On a quarterly basis, the air conditioning systems undergo an inspection from a third-party specialist to help ensure that the equipment is in proper working order. The facilities are equipped with multiple UPS systems and diesel generators to provide electricity in the event of a power outage. The data centers also contain two distinct electrical connections to the electrical company's substation. Utility power is run through the UPS battery systems so that customers receive clean, conditioned battery power. In the event that a loss of utility power occurs, the generators will engage and begin supplying power to the UPS systems. Whether it is from utility or generator power, each customer draws power from the UPS battery systems, ensuring smooth transitions from utility to generator and back again. On a semi-annual basis, UPS inspections are performed, and on a quarterly basis, generator inspections are performed to help ensure that the systems are in proper working order. Additionally, internal personnel perform preventative maintenance procedures on the UPS systems and generators on a quarterly basis.

Malicious Software Management

Windows production servers and workstations are configured with CrowdStrike antivirus software which is configured to scan for updates to antivirus definitions and update signatures on a real-time basis and has on-access scanning of executables and files.

Change Management

Infrastructure changes follow formal change control procedures to help ensure that only tested (when applicable) and authorized changes are implemented. Change control procedures include:

- **Identification and recording of significant changes;**
- **Planning and testing of changes;**
- **Assessment of the potential impacts, including security impacts, of such changes;**
- **Formal approval procedure for proposed changes from system or business owners;**
- **Communication of change details to relevant persons; and**
- **Audit trail of changes.**

Changes are documented in ticketing systems with requirements for specific mandatory fields to be completed to perform risk assessments and to enable effective coordination and communication within the change process. IT management will review the ticket and provide their approval or rejection based on the change request. Changes are required to be tested prior to being implemented and post implementation to help ensure there is no adverse effect or impact on the system. Change control documentation reflects an audit trail of the change including the date and time of change, reason for change, the name of the person making the change, and the person or persons who authorized the change.

The ability to implement infrastructure changes is restricted to user accounts granted permissions and group assignments assigned to authorized executive management, IT, and NetOps personnel. Change management meetings are held on a weekly basis to discuss and communicate the ongoing and upcoming infrastructure changes and projects affecting the system. Meeting minutes are retained and approval for upcoming changes by the Change Advisory Board are documented within the respective change request ticket.

Disaster Recovery

Business resiliency plans, including disaster recovery plans, and contingency plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event. The plans include roles and responsibilities, recovery time objectives (RTO), procedures for various scenarios, and task checklists in the event of an emergency. Additionally, disaster recovery tests are performed on an annual basis. The results of the annual disaster plan are recorded and tracked to identify and monitor potential threats to the critical infrastructure supporting the Colocation Services.

Ongoing Monitoring

The entity's IT security group monitors the security impact of emerging technologies, and the impact of applicable laws or regulations are considered by senior management. Ongoing monitoring consists of IT personnel receiving e-mail notifications and subscriptions, as well as following blogs to stay informed of the latest IT trends which could affect system security and availability. IT security personnel utilize a third-party utility to perform a vulnerability scan of the production servers on a monthly basis to identify threats and assess their potential impact to the production environment. Any security vulnerabilities that are identified are triaged by IT security personnel and monitored through resolution.

Capacity and Availability Monitoring

Switch has implemented an internally developed custom built application called SYSLOG to monitor the network devices' capacity and availability levels (e.g., central processing unit (CPU) levels, uptime, etc.) and alert operations personnel when predefined thresholds have been met. Switch uses an enterprise monitoring tool to log and monitor network availability and security incidents.

On-call personnel are notified via e-mail by SYSLOG of availability issues that exceed predefined thresholds on monitored network devices. The NOC is staffed on a 24 hour a day on-call basis to respond to availability issues. Additionally, operations meetings are held on a weekly basis to review availability trends and availability forecasts as compared to system commitments.

Incident Response

The network infrastructure is monitored 24 hours per day by NOC technicians to assist with network issues and to respond to customer inquiries and incidents. Management has implemented procedures to guide NOC technicians in identifying and responding to network related incidents, as well as incident response and escalation procedures in the event that an event is detected, to provide timely and consistent communication to the business and customers.

A proprietary ticketing system, LDC, was developed and is utilized to handle network related issues in order to manage, track, and respond to network issues until resolution. When an issue is detected, NOC technicians will examine the issue and create a ticket to assign priority level on a scale (1-5) based on the urgency and impact of the incident to the business and/or the customer, and to determine predefined timelines to resolve the issue. If the ticket is not responded to within a predefined timeline based on its severity, the ticketing system is configured to notify NOC technicians of the open ticket until the ticket is addressed. Incidents identified by customers can be communicated to the NOC by phone, e-mail, or on the LDC portal.

If the issue cannot be resolved within the predefined timeline, escalation procedures have been implemented for the assigned NOC technician to notify the responsible department and/or vendor through a predetermined set of contacts. Once the affected departments have been notified of the issue, e-mail updates are sent out to the business or customers on an as needed basis until the issue is resolved. Once the issue is fixed, the NOC technician will update the support ticket with full details of the issue resolution and close the ticket. Additionally, management meetings are held on a biweekly basis to discuss incidents and corrective measures to help ensure that incidents are resolved.

Data

Badge access logs and video surveillance recordings are a key component of the Colocation Services provided by Switch. The logs and recordings are reviewed on a real-time basis by SECOM and retained for forensic purposes. Customer data was not included in the scope of this examination as Switch is not responsible for the administration or maintenance of customer systems or data.

Subservice Organizations

No subservice organizations were relevant to the scope of this assessment whose controls were necessary, in combination with controls at Switch, to provide reasonable assurance that Switch's service commitments and system requirements were achieved.

Complementary Controls at User Entities

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

Trust Services Criteria Not Applicable to the In-Scope System

All criteria within the security and availability categories are applicable to the Switch Colocation Services system.