HITRUST
6175 Main Street
Suite 400
Frisco, TX 75034

October 31, 2023

Switch Ltd.
PO Box 400850
Las Vegas, Nevada 89140-0850

Based upon representation from management as to the accuracy and completeness of information provided, the procedures performed by an Authorized External Assessor to validate such information, and HITRUST's independent confirmation that the work was performed in accordance with the HITRUST® Assurance Program requirements, the following platforms, facilities, and supporting infrastructure of the Organization ("Scope") meet the HITRUST CSF® v9.3 Risk-based, 2-year (r2) certification criteria:

Platforms:

- C-Cure Badge Access System residing at ATL 1 Data Center Facility (ATL1), GRR 1 Data Center Facility (GRR1), LAS 10 Data Center Facility (LAS10), LAS 11 Data Center Facility (LAS11), LAS 12 Data Center Facility (LAS12), LAS 15 Data Center Facility (LAS15), LAS 2 Data Center Facility (LAS2), LAS 4 Data Center Facility (LAS4), LAS 5 Data Center Facility (LAS5), LAS 7 Data Center Facility (LAS7), LAS 8 Data Center Facility (LAS8), LAS 9 Data Center Facility (LAS9), RNO 1 Data Center Facility (RNO1), and RNO 2 Data Center Facility (RNO2)
- Cisco Border and Private Routers residing at ATL 1 Data Center Facility (ATL1), GRR 1 Data Center Facility (GRR1), LAS 10 Data Center Facility (LAS10), LAS 11 Data Center Facility (LAS11), LAS 12 Data Center Facility (LAS12), LAS 15 Data Center Facility (LAS15), LAS 2 Data Center Facility (LAS2), LAS 4 Data Center Facility (LAS4), LAS 5 Data Center Facility (LAS5), LAS 7 Data Center Facility (LAS7), LAS 8 Data Center Facility (LAS8), LAS 9 Data Center Facility (LAS9), RNO 1 Data Center Facility (RNO1), and RNO 2 Data Center Facility (RNO2)
- Living Data Center (LDC) residing at LAS 9 Data Center Facility (LAS9)
- Microsoft Active Directory Domain residing at ATL 1 Data Center Facility (ATL1), GRR 1 Data Center Facility (GRR1), LAS 10 Data Center Facility (LAS10), and RNO 1 Data Center Facility (RNO1)

Facilities:

- LAS 15 Data Center Facility (LAS15) (Data Center) located in Las Vegas, Nevada, United States of America

- LAS 12 Data Center Facility (LAS12) (Data Center) located in Las Vegas, Nevada, United States of America
- LAS 11 Data Center Facility (LAS11) (Data Center) located in Las Vegas, Nevada, United States of America
- LAS 10 Data Center Facility (LAS10) (Data Center) located in Las Vegas, Nevada, United States of America
- LAS 9 Data Center Facility (LAS9) (Data Center) located in Las Vegas, Nevada, United States of America
- LAS 8 Data Center Facility (LAS8) (Data Center) located in Las Vegas, Nevada, United States of America
- LAS 7 Data Center Facility (LAS7) (Data Center) located in Las Vegas, Nevada, United States of America
- LAS 5 Data Center Facility (LAS5) (Data Center) located in Las Vegas, Nevada, United States of America
- LAS 4 Data Center Facility (LAS4) (Data Center) located in Las Vegas, Nevada, United States of America
- LAS 2 Data Center Facility (LAS2) (Data Center) located in Las Vegas, Nevada, United States of America
- RNO 2 Data Center Facility (RNO2) (Data Center) located in McCarran, Nevada, United States of America
- RNO 1 Data Center Facility (RNO1) (Data Center) located in McCarran, Nevada, United States of America
- GRR 1 Data Center Facility (GRR1) (Data Center) located in Grand Rapids, Michigan, United States of America
- ATL 1 Data Center Facility (ATL1) (Data Center) located in Lithia Springs, Georgia, United States of America

The certification is valid for a period of two years assuming the following occurs. If any of these criteria are not met, HITRUST will perform an investigation to determine ongoing validity of the certification and reserves the right to revoke the Organization's certification.

- No data security breach reportable to a federal or state agency by law or regulation has occurred within or affecting the assessed environment,

- No significant changes in the business or security policies, practices, controls, and processes have occurred that might impact its ability to meet the HITRUST Risk-based, 2-year (r2) certification criteria, and

- Timely completion of the HITRUST Interim Assessment for r2 Certification as defined in the HITRUST Assurance Program Requirements.

HITRUST has developed the HITRUST CSF, a certifiable framework that provides organizations with the needed structure, detail and clarity relating to information protection. With input from

HITRUST
6175 Main Street
Suite 400
Frisco, TX 75034

leading organizations, HITRUST identified a subset of the HITRUST CSF controls that an organization must meet to be HITRUST Risk-based, 2-year (r2) Certified.

HITRUST performed a quality assurance review to ensure that the control maturity scores were consistent with the results of testing performed by the Authorized External Assessor. Users of this letter can refer to the document Leveraging HITRUST Assessment Reports: A Guide for New Users for questions on interpreting this letter and can contact HITRUST customer support at support@hitrustalliance.net. Users of this letter are assumed to be familiar with and understand the services provided by the organization listed above, and what specific services are being used by the user organization.

A version of this letter with a more detailed scope description has also been issued by HITRUST which can also be requested from the organization listed above directly. A full HITRUST Validated Assessment Report has also been issued by HITRUST which can also be requested from the organization listed above directly. Additional information on the HITRUST Assurance Program can be found at the HITRUST website at https://hitrustalliance.net.

HITRUST

HITRUST

December 5, 2022

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, 2021 through September 30, 2022, 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 2022, 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, 2022, 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. Phone: 702-444-4116 Fax 866-518-2436
POB 400850, Las Vegas, Nevada 89140

SOC 1 REPORT

FOR

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, 2020, TO SEPTEMBER 30, 2021

PREPARED IN ACCORDANCE WITH THE
AICPA SSAE NO. 18 AND IAASB ISAE 3402 STANDARDS

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 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

schellman

INDEPENDENT SERVICE AUDITOR'S REPORT

To Switch, Ltd.:

Scope

We have examined Switch, Ltd.'s ("Switch" or "service organization") description of its Colocation Services system throughout the period October 1, 2020, to September 30, 2021 (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 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.

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. 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, 2020, to September 30, 2021. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- Performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on the criteria in management's assertion;
- Assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description;

- Testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved; and
- Evaluating the overall presentation of the description, suitability of the control objectives stated in the description, and suitability of the criteria specified by the service organization in its assertion.

Service Auditor's Independence and Quality Control

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

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in processing or reporting transactions in providing the 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 Colocation Services system that was designed and implemented throughout the period October 1, 2020, to September 30, 2021;

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, 2020, to September 30, 2021, 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, 2020, to September 30, 2021; 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, 2020, to September 30, 2021, 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, 2020, to September 30, 2021.

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, 2020, to September 30, 2021, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatement of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than the specified parties.

Schellman & Company, LLC

Tampa, Florida
November 8, 2021

SECTION 2

MANAGEMENT'S ASSERTION

MANAGEMENT'S ASSERTION

We have prepared the description of Switch, Ltd.'s ("Switch") Colocation Services system for user entities' of the system throughout the period October 1, 2020, to September 30, 2021 (the "description"), for user entities of the system during some or all of the period October 1, 2020, to September 30, 2021, 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 Colocation Services system made available to user entities of the system during some or all of the period October 1, 2020, to September 30, 2021, for providing Colocation Services. The criteria we used in making our 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 and 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 Colocation Services system during the period covered by the description; and

   iii. does not omit or distort information relevant to the scope of the 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

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, 2020, to September 30, 2021, 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, 2020, to September 30, 2021. 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 750 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 all 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 virtually unlimited 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 rich technology ecosystem that benefits its participants. Switch continues to further enhance these benefits as they innovate and expand their platform ecosystem. Switch currently has more than 940 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 twelve colocation facilities with an aggregate of nearly 5 million gross square feet (GSF) of space. These facilities have up to 454 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 our advanced colocation facilities while reducing exposure to the 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 our enterprise customers.

As additional locations and sectors within our 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 considerable. 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 man-trap relay logic. Each man-trap includes fixed cameras viewing every door.

Every customer space, whether it is a cage, cabinet, or suite, is individually locked, protected, and monitored. Additional security safeguards, such as man-traps, 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 every person 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 HD with automatic low-light switching, capable of viewing up to .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. IOU provides a better use of the system to include constant monitoring, use of the 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 currentASIS 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 state-of-the-art environmental controls to protect the systems of its customers as well as operating in the most energy-efficient means possible. 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, capable and 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 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.

Boundaries of the System

The scope of this report is limited to the Colocation Services for the Las Vegas 2, Las Vegas 4, Las Vegas 5, Las Vegas 7, Las Vegas 8, Las Vegas 9, Las Vegas 10, Las Vegas 11, and Las Vegas 12 facilities located in Las Vegas, Nevada, as well as, the single Colocation Services facilities located in Reno, Nevada, Grand Rapids, Michigan, and Atlanta, Georgia. 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 document.

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.

Subservice Organizations

No subservice organizations were included in 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 Review Period

No significant changes to the Colocation Services system occurred during the review period.

Functional Areas of Operations

Switch utilizes specific functional areas of operations that support the scope of this review, these 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) department – 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.**
- **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.**

Infrastructure

The in-scope infrastructure supporting the Colocation Services is included in the table below:

Primary Infrastructure			
Production Application	**Business Function Description**	**Operating System Platform**	**Physical Location**
The Living Data Center 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.	Microsoft 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.	Microsoft Windows	
C-Cure Badge Access System	Physical access control supporting the Colocation Services at the Las Vegas and Atlanta facility.		

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

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.

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 directors and operations management.

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of 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 include:

- 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 Directors and Audit Committee Oversight

Switch's control consciousness is influenced significantly by its Owners and Board of Directors' participation. A Board of Directors 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 appropriate 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 appropriate 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 appropriate 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 services provided.
- Management meetings are held on a periodic basis to discuss operational issues.

Switch's human resources 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 on-boarding 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 acknowledgement of receipt of employee handbook document; and
    - Verification that the employee has taken security training and signed an acknowledgement 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 the management's description of the services organizations systems. 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 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 are 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 Directors 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 code of conduct, entity values and behavioral standards. Employees are required to sign an acknowledgement form 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 requires employees to complete a training program to help ensure that employees have the necessary training to carry out their responsibility.

Human Resource Management

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

Switch has documented policies and procedure for employee on-boarding and off-boarding. 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 acknowledgement 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 for 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 (i.e., 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. Pre-defined access groups are utilized to provide access depending on the individual's role and responsibilities. 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 man-trap where they must scan the badge access card and provide biometric credentials. 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 ad-hoc 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 ad-hoc review. The facilities are monitored 24 hours per day by security personal with the use of motion sensitive digital surveillance cameras, alarms, and motion detectors. 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.

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 pre-defined thresholds are exceeded.

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. Utility power is run through the UPS battery systems so that customers are always receiving 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 is always drawing power from the UPS battery systems, ensuring smooth transitions from utility to generator and back again. On an annual basis, a third-party specialist inspects the UPS systems and generators to help ensure that the systems are in proper working order. 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. 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: Controls 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 called Living Data Center 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 pre-defined 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 Living Data Center customer portal. NOC personnel will verify the request was initiated by an authorized customer contact. In the event that the request was initiated by an unauthorized customer, NOC personnel will 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 Living Data Center 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 a regular basis until the issue is resolved.

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 will be 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 will then schedule a new customer welcome call. During this call the members of the IT and operations groups will go over the customer cage or cabinet set up and provide the customer with and the 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
- AT&T
- ATT Michigan (Michigan Bell Telephone Company)
- Bandwidth Infrastructure Group (BIG)
- Casair
- CC Communications
- Charter
- Cogent
- Comcast
- Cox
- Crown Castle (former Wilcon)
- Everstream (former Comlink)
- GTT
- IX Reach
- Lumen
- Masergy
- Megaport
- Packet Fabric
- Parker Fiber
- PCCW
- Roberts
- Sky Fiber
- Tata
- Telepacific
- Time Warner Cable
- T-Mobile (former 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 the company'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 Living Data Center (LDC) system for overall monitoring. The platform includes an incident ticketing system as well as real-time monitoring capabilities referred to as the Living Data Center. 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 semi-annual 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 make 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 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 was restricted to the 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, 2020, through September 30,2021.

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 review 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.

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 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 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, 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 appropriate lines of reporting.	No exceptions noted.
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 communicated entity values and behavioral standards to personnel.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.03	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.	Inspected the employee handbook acknowledgment form for a sample of employees hired during the reporting period to determine that policies and procedures require that employees sign an acknowledgement form 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 for each employee sampled.	No exceptions noted.
1.04	Management ensures that employees have adequate training to carry out their job responsibilities.	Inspected the training expenditures during the reporting period and the departmental training materials to determine that that employee had adequate training material to carry out their job responsibilities.	No exceptions noted.
1.05	A board of directors is in place to oversee management activities.	Inquired of management regarding the board of directors to determine that a board of directors was in place to oversee management activities.	No exceptions noted.
		Observed the meeting minutes for a sample of board of directors' meetings held during the reporting period to determine that a board of directors was in place and met during the reporting period.	No exceptions noted.

HUMAN RESOURCES MANAGEMENT

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that employee onboarding and off-boarding 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 evidence of completed background screening for a sample of employees hired during the reporting 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 evidence of completed drug screening tests for a sample of employees hired during the reporting 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 agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.	Inspected the signed confidentiality statements for a sample of employees hired during the reporting period to determine that each employee sampled signed a confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.	No exceptions noted.
2.04	Employees, customers, and vendors must undergo orientation 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, customer, and vendors must undergo orientation to help 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 customer security orientation materials, the information security orientation acknowledgements with respect to the information security policy, and the arc flash safety procedures and evidence of completed training for a sample of employees hired during the reporting period to determine that employees, customers, and vendors must undergo orientation to help ensure that security and safety requirements were communicated.	No exceptions noted.
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 badge access and system privileges for a sample of employees terminated during the reporting period to determine that access and system privileges to systems were revoked for each terminated 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.
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 and addressed 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 user access privileges to determine that the ability to create, modify, or delete user badge access privileges to the facilities was restricted to user accounts accessible by persons 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 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 Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the results of the most recently completed semi-annual user access review to determine that a full review of employee and customer access privileges was performed during the review 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 privileges and zone definitions to determine that badge access card privileges were assigned to users using predefined access zones to help ensure that access privileges were consistently assigned based on job responsibilities and/or where customer equipment was located.	No exceptions noted.
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 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 badge access privileges for a sample of employees terminated during the review period to determine that badge access privileges were revoked for each terminated 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 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 Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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 director of IT regarding the visitor sign-in process to determine that visitors were required to 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 to determine that visitors were required to present a picture identification card, which was either retained or digitally scanned, and were escorted 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 granting of access.	Inspected the physical access request approvals for a sample of employees and contractors granted access during the review period to determine that physical access to the data center was documented and approved by the employee's manager prior to granting of access 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 director of IT regarding access within the in-scope facilities to determine that personnel at the facilities were distinguished as being one of the following: • Employees with badge access cards • Customers with badge access cards • Contractors with badge access cards • Visitors with non-functioning visitor badges	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 has red-colored badges but wear 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 man-trap 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 in-scope data centers entrance process to determine that personnel and authorized customers and contractors were required to enter a man-trap 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.	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 access within the in-scope data centers 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 visitor access procedures to determine that visitors without badge access cards were escorted while within the facilities.	No exceptions noted.
		Inspected the access control policy to determine that visitors were required to be 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
3.16	Physical access to the customer cages is documented and approved by the customer prior to granting of access.	Inspected the physical access request approvals to the customer cages for a sample of vendors and customers granted access during the review period to determine that physical access to the customer cages was documented and approved by the customer prior to granting of access 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 director of IT 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 a sample of activity logs recorded during the review period to determine that the following attributes for physical movements within the facilities were captured and maintained during the review 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 security command center to determine that digital surveillance video cameras recorded activities at facility entrances, the building perimeters, and other areas within the facilities.	No exceptions noted.
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.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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 in-scope data centers 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 the facilities entrances and manage visitor access 24 hours per day.	Observed the security personnel at the security command center to determine that security personnel monitored access to the facilities and managed visitor access.	No exceptions noted.
		Inspected the master shift schedule for security personnel to determine that security personnel were staffed to monitor access to the facilities on a 24 hour per day basis during the review period.	No exceptions noted.
3.22	Security personnel utilize an incident reporting system to document any physical security incidents.	Inspected a recent incident report to determine that security personnel utilized an incident reporting system to document any physical security incidents during the review 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 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 information technology 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 formal 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 in-scope data center 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 director of IT regarding fire suppression to determine that the dual-interlock (pre-action) dry pipe water sprinklers required both a smoke detection event and the activation of sprinklers to release water into the pipes.	No exceptions noted.
		Observed the in-scope data center facilities to determine that the data centers were equipped with pre-action water sprinklers.	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 systems inspection reports for a sample of quarters during the review period to determine that the business process director obtained inspection reports as evidence 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 systems inspection reports for a sample of quarters during the review period to determine that the business process director obtained inspection reports as evidence 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 current inspection tags for a sample of hand-held fire extinguishers to determine that the business process director obtained inspection tags as evidence that each hand-held fire extinguisher sampled underwent maintenance inspections during the review 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 guided 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 director of IT regarding the monitoring of temperature and humidity levels to determine that operations personnel monitored temperature and humidity levels and that identified issues were responded to as necessary.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the monitoring system configurations 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 within the in-scope data centers to determine that the data centers utilized redundant air conditioning units.	No exceptions noted.
		Observed the server farm layout to determine that that 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 to determine that the devices were 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 systems inspection reports for a sample of quarters during the review period to determine that the business process director obtained inspection reports as evidence 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 systems inspection reports for a sample of quarters during the review period 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 for in-scope data centers 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 presence of the UPS systems for in-scope data centers 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 e-mail notification generated during the review 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 reports for a sample of quarters during the review period to determine that the business process director obtained inspection reports as evidence 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 at a monthly basis.	Inspected the generator inspection reports for a sample of months during the review period to determine that internal personnel performed preventative maintenance procedures on the generators for each month sampled.	No exceptions noted.
4.17	The business process director obtains inspection reports as evidence that the UPS systems undergo maintenance inspections on an annual basis.	Inspected the most recent UPS systems inspection reports to determine that the business process director obtained inspection reports as evidence that the UPS systems underwent maintenance inspections during the review period.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
4.18	Internal personnel perform preventative maintenance procedures on the UPS systems on a semi-annual basis.	Inspected the most recent semi-annual UPS systems inspection reports to determine that internal personnel performed preventative maintenance procedures on the UPS systems during the review period.	No exceptions noted.
4.19	The data centers contain two distinct electrical connections to the electrical company's substation.	Inquired of the director of IT regarding electric connectivity to determine that the data centers contained two distinct electrical connections to the electrical company's substation.	No exceptions noted.
		Observed the power connections to the facilities to determine that the facilities 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 pre-defined 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 pre-defined list of IP addresses.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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 help 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.
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 authentication 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.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
5.07	Authentication parameters for the centralized authentication system are derived from the corporate network domain controller.	Inspected the centralized authentication system authentication 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.
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 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 review period.	No exceptions noted.
		Inspected the centralized authentication system logging configurations and example logs generated during the review 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: Controls 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	Documenting 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 routers were configured for redundancy such that if one failed, network connectivity was still available to customers for each router sampled.	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 applications' configurations and example e-mail alert notifications generated during the reporting 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.	Inspected the NOC staffing schedules for a sample of weeks during the reporting 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 an example ticket resolved during the reporting period to determine that operations personnel utilized a ticketing system to track the status of incidents and service disruptions.	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 • Priority • Problem type • Description of event • Correspondence with customers • Resolution details	**Inspected a sample of incident tickets recorded during the reporting period to determine that each ticket sampled included the following:** • Date and time of the incident • Priority • 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 operations personnel configure priority ratings for tickets created by the ticketing system 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 pre-defined 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 director of IT compliance 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 schedules for a sample of weeks during the review period to determine that the NOC was staffed 24 hours per day for each week sampled.	No exceptions noted.
7.04	Operations personnel utilize a ticketing system to track the status of incidents and service disruptions.	Inspected the ticketing system dashboard and example incident ticket resolved during the review period to determine that operations personnel utilized a ticketing system to track the status of incidents and service disruptions.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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 • Priority • Problem type • Description of event • Correspondence with customers • Resolution details	**Inspected a sample of incident tickets recorded during the review period to determine that each ticket sampled included the following:** • **Date and time of the incident** • **Priority** • **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 queries to determine that the ticketing system is configured for NOC personnel to perform real-time monitoring of open tickets that have 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 information technology and operations personnel in the customer provisioning process.	Inspected the customer provisioning policies and procedures and customer provisioning thank you template to determine that documented policies and procedures were in place to guide information technology and operations personnel in the customer provisioning process.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
8.02	Operations personnel require a customer service agreement to be executed in order to begin the implementation process.	Inspected the executed service agreements for a sample of customers provisioned during the reporting period to determine that operations personnel require a customer service agreement to be executed in order to begin the implementation process.	No exceptions noted.
8.03	A completed engineering document and client contact form is required prior to the provisioning process that include, but is not limited to, the following: • Contact information • Network connectivity requirements • Network redundancy requirements • Customer cabinet layout	**Inquired of the director, IT compliance regarding customer implementations to determine that a completed engineering document and client contact form was obtained prior to the provisioning process 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 reporting period to determine that a completed provisioning questionnaire was obtained for each customer sampled.	No exceptions noted.
8.04	Members of the information technology 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, IT compliance, regarding customer implementations to determine that members of the information technology and operations groups conducted a new customer welcome call with new customers to review requested settings to help ensure that the services to be provisioned matched the customer's expectations.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected evidence of new customer welcome calls for a sample of customers provisioned during the reporting period to determine that members of the information technology 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.	No exceptions noted.

SWITCH, LTD.

SOC 2 REPORT

FOR

COLOCATION SERVICES

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

OCTOBER 1, 2020, TO SEPTEMBER 30, 2021

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

Attestation and Compliance Services

This report is intended solely for use by the management of 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 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

schellman

INDEPENDENT SERVICE AUDITOR'S REPORT

To Switch, Ltd.:

Scope

We have examined Switch, Ltd.'s ("Switch" or the "service organization") accompanying description of its Colocation Services system, in Section 3, throughout the period October 1, 2020, to September 30, 2021, (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, 2020, to September 30, 2021, 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; and
- Evaluating the overall presentation of the description.

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

Service Auditor's Independence and Quality Control

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

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

Inherent Limitations

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

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

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

Description of Test of Controls

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

Opinion

In our opinion, in all material respects:

a. the description presents Switch's Colocation Services system that was designed and implemented throughout the period October 1, 2020, to September 30, 2021, in accordance with the description criteria;

b. the controls stated in the description were suitably designed throughout the period October 1, 2020, to September 30, 2021, 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 review period; and

c. the controls stated in the description operated effectively throughout the period October 1, 2020, to September 30, 2021, 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, 2020, to September 30, 2021, business partners of Switch subject to risks arising from interactions with the Colocation Services system, practitioners providing services to such user entities and business partners,

prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization;
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties;
- Internal control and its limitations;
- 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 18, 2021

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, 2020, to September 30, 2021, (the "description") based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), ("description criteria"). The description is intended to provide report users with information about the Colocation Services system that may be useful when assessing the risks arising from interactions with 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, 2020, to September 30, 2021, in accordance with the description criteria;

b. the controls stated in the description were suitably designed throughout the period October 1, 2020, to September 30, 2021, 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, 2020, to September 30, 2021, 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 Chief Executive Officer (CEO), Rob Roy, has developed more than 750 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 all 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 virtually unlimited 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 rich technology ecosystem that benefits its participants. Switch continues to further enhance these benefits as they innovate and expand their platform ecosystem. Switch currently has more than 940 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. We believe that traditional technology infrastructure is not capable of supporting the growing wave of mission critical data and increasingly powerful information technology (IT) equipment.

Switch presently owns and operates four primary campus locations, called Primes, which encompass twelve colocation facilities with an aggregate of nearly 5 million gross square feet (GSF) of space. These facilities have up to 454 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 our advanced colocation facilities while reducing exposure to the 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 our enterprise customers.

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

[Intentionally Blank]

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 considerable. 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 man-trap relay logic. Each man-trap includes fixed cameras viewing every door.

Every customer space, whether it is a cage, cabinet, or suite, is individually locked, protected, and monitored. Additional security safeguards, such as man-traps, 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 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 every person 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 HD with automatic low-light switching, capable of viewing up to .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. IOU provides a better use of the system to include constant monitoring, use of the 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 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 state-of-the-art environmental controls to protect the systems of its customers as well as operating in the most energy-efficient means possible. 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, capable and 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 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 Colocation Services. Those objectives are based on the service commitments that Switch makes to user entities, the laws and regulations that govern the provision 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 security 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 confidentiality policies. Commitments and requirements of Switch are documented in customer contracts and are updated and signed upon any changes in the confidentiality practices.

In accordance with our 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 Las Vegas 2, Las Vegas 4, Las Vegas 5, Las Vegas 7, Las Vegas 8, Las Vegas 9, Las Vegas 10, Las Vegas 11, Las Vegas 12 facilities located in Las Vegas, Nevada as well as the single Colocation Services facilities located in Reno, Nevada, Grand Rapids, Michigan and Atlanta, Georgia.

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.

Infrastructure and Software

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

Primary Infrastructure			
Production Application	**Business Function Description**	**Operating System Platform**	**Physical Location**
The Living Data Center 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.	Microsoft 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.	Microsoft Windows	
C-Cure Badge Access System	Physical access control supporting the Colocation Services at the Las Vegas and Atlanta facilities.		

In addition, Switch utilizes Sophos antivirus software for antivirus protection for the Windows production servers and workstations. Furthermore, Switch utilizes both the Honeywell MAXPRO Video Management System (VMS) and the Milestone 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, these 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) department – 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.

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 will detail the specific production systems and required levels of access privileges. When an employee ends their employment, a termination checklist is completed to document the off-boarding 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 data center facilities. Pre-defined access groups are utilized to provide access depending on the individual's role and responsibilities. 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 man-trap where they must scan the badge access card and provide biometric credentials. 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 ad-hoc 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 ad-hoc review. The facilities are monitored 24 hours per day by security personal with the use of motion sensitive digital surveillance cameras, alarms, and motion detectors. 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.

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 pre-defined thresholds are exceeded.

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. Utility power is run through the UPS battery systems so that customers are always receiving 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 is always drawing

power from the UPS battery systems, ensuring smooth transitions from utility to generator and back again. On an annual basis, a third-party specialist inspects the UPS systems and generators to help ensure that the systems are in proper working order. 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 Sophos antivirus software which is configured to scan for updates to antivirus definitions and update signatures on an hourly basis and on-access scanning of executables and files.

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.

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 only those personnel responsible for those activities via user account permissions and group assignments.

Disaster Recovery

Disaster recovery plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event. Disaster recovery tests are performed on an annual basis, and the results were recorded and tracked to identify potential threats.

Incident Response

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 called Living Data Center (LDC) was developed and is utilized to manage, track, respond, and resolve network issues. 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.

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 resolution.

Capacity and Availability Monitoring

SYSLOG is configured to monitor the network devices' capacity and availability levels (e.g. CPU levels, uptime, etc.) and alert operations personnel when predefined thresholds have been met. The NOC is staffed on a 24 hour a day on-call basis to respond to availability issues.

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

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 Review Period

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

Subservice Organizations

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.

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 directors and operations management.

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of 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 include:

- **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 checks 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 Directors and Audit Committee Oversight

Switch's control consciousness is influenced significantly by its Owners and Board of Directors' participation. A Board of Directors 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 services provided.**
- **Management meetings are held on a periodic basis to discuss operational issues.**

Switch's human resources 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 on-boarding 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 acknowledgement of receipt of employee handbook document; and**
  - **Verification that the employee has taken security training and signed an acknowledgement of such training.**
- **Management utilizes termination procedures which include, but are not limited to, the following elements:**
  - **Collection of company property;**
  - **Revocation of physical access rights;**
  - **Revocation of system access rights;**
  - **Signatures of each person that performs requisite tasks; and**
  - **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 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; 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 Factors

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 are applicable to the 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
- AT&T
- ATT Michigan (Michigan Bell Telephone Company)
- Bandwidth Infrastructure Group (BIG)
- Casair
- CC Communications
- Charter
- Cogent
- Comcast
- Cox
- Crown Castle (former Wilcon)
- Everstream (former Comlink)
- GTT
- IX Reach
- Lumen
- Masergy
- Megaport
- Packet Fabric
- Parker Fiber
- PCCW
- Roberts
- Sky Fiber
- Tata
- Telepacific
- Time Warner Cable
- T-Mobile (former 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.

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 the company'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 for overall monitoring. The platform includes an incident ticketing system as well as real-time monitoring capabilities referred to as the Living Data Center. 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 semi-annual security assessments in accordance with the Department of Homeland Security (DHS) Argonne model.

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 make 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

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

SECTION 4

TESTING MATRICES

TESTS OF OPERATING EFFECTIVENESS AND RESULTS OF TESTS

Scope of Testing

This report on the controls relates to the Colocation Services system provided by Switch. The scope of the testing was restricted to the Colocation Services system and its boundaries as defined in Section 3. Schellman conducted the examination testing over the period October 1, 2020, to September 30, 2021.

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 review 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 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 review period to determine that an acknowledgment form 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 had been signed by each employee sampled.	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 evidence of completed background checks for a sample of employees hired during the review 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 evidence of completed drug screening tests for a sample of employees hired during the review 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 agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.	Inspected the signed confidentiality statements for a sample of employees hired during the review period to determine that a confidentiality statement was signed by each employee sampled.	No exceptions noted.
CC1.1.5	An employee sanction policy is in place that address 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 address 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 directors 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 directors established and maintained a formal charter and set of bylaws which describes 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 most recent nominating and corporate governance committee meeting minutes to determine that external board members attest to their independence from management and objectivity in evaluations and decision making on an annual basis.	No exceptions noted.
CC1.2.3	Board of directors 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 directors meeting minutes for a sample of quarters to determine that board of directors 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 directors 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 directors meeting minutes for a sample of quarters to determine that board of directors 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 VP of Human Resources 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 appropriate 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 descriptions for job positions to determine that documented position descriptions were in place to define the skills, responsibilities, and knowledge levels required for particular jobs for each job position sampled.	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 security operations, data center operations, and network operations 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 security operations, data center operations, and network operations 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 checklists for a sample of employees hired during the review 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 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 verification that candidates possess 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 reporting period and the departmental training materials to determine that employees had adequate training material to carry out their job responsibilities.	No exceptions noted.
CC1.4.4	Employees, customers, and vendors must undergo orientation 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, customer, and vendors must undergo orientation to help ensure that security and safety requirements were communicated.	No exceptions noted.
		Inspected the security orientation materials to determine that orientation included the following: • 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 orientation acknowledgements with respect to the information security policy for a sample of employees hired during the reporting period to determine that each employee sampled acknowledged their responsibilities with respect to information security.	No exceptions noted.
		Inspected the arc flash safety procedures and evidence of completed training for a sample of employees hired during the review period to determine that each employee sampled completed electrical system safety training.	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 current employees to determine that each employee sampled completed security awareness training during the review 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 VP of Human Resources 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 appropriate 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 descriptions for a sample of job positions to determine that documented position descriptions were in place to define the skills, responsibilities, and knowledge levels required for particular jobs for each job position sampled.	No exceptions noted.
CC1.5.3	An employee sanction policy is in place that address 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 address 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
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 invite, example meeting notes, and the information security policy to determine that management formally documented 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.	No exceptions noted.
CC1.5.5	Board of directors 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 directors meeting minutes for a sample of quarters to determine that board of directors 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 identifies information required to support the functioning of internal control and achievement of objectives and associated protection and access rights.	No exceptions noted.
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 applications' configurations and example e-mail alert notifications generated during the review 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 the facilities entrances and manage visitor access 24 hours per day.	Inspected the master shift schedule for security personnel to determine that security personnel were staffed to monitor access to the facilities on a 24 hour per day basis during the review period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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 director of IT regarding the monitoring of temperature and humidity levels to determine that operations personnel monitored temperature and humidity levels and that identified issues were responded to as necessary.	No exceptions noted.
		Inspected the monitoring system configurations to determine that the data centers' temperature and humidity levels were systematically monitored and that the monitoring system was configured to notify personnel 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 to determine that the data center power levels were systematically monitored and that the monitoring system was configured to alert personnel when predefined minimum and maximum thresholds were exceeded.	No exceptions noted.
		Inspected example security update e-mail notification received during the review period to determine that the entity's IT security group monitored the security impact of emerging technologies.	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 that it was communicated to internal and external users.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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 and company intranet site 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 current employees to determine that each employee sampled completed security awareness training during the review period.	No exceptions noted.
CC2.2.4	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.	Inspected the employee handbook acknowledgment form for a sample of employees hired during the review period to determine that an acknowledgment form 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 had been signed by each employee sampled.	No exceptions noted.
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, company intranet site, and 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.	Inquired of the director, IT compliance regarding change management meetings to determine that change management meetings were held on a weekly basis to discuss and communicate the ongoing and upcoming projects that affected the system.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the recurring calendar meeting invitation, agenda, and minutes for a sample of weeks during the review period to determine that change management meetings were held to discuss and communicate the ongoing and upcoming projects that affect the system for each week sampled.	No exceptions noted.
CC2.2.7	Management meetings are held on a weekly basis to discuss incidents and corrective measures to help ensure that incidents are resolved.	Inquired of the director, IT compliance, regarding management meetings to determine that management meetings were held on a weekly basis to discuss incidents and corrective measures to help ensure that incidents were resolved.	No exceptions noted.
		Inspected the management meeting minutes for a sample of weeks during the review 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 descriptions for a sample of job positions to determine that documented position descriptions were in place to define the skills, responsibilities, and knowledge levels required for particular jobs for each job position sampled.	No exceptions noted.
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 that it was communicated to internal and external users.	No exceptions noted.
CC2.3.2	The entity's security and availability commitments and the associated system requirements are documented in customer contracts.	Inspected a standard executed service agreement for an example customers provisioned during the review period to determine that the entity's security and availability commitments and the associated system requirements were documented in customer contracts.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.3.3	Members of the information technology 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, IT compliance, regarding customer implementations to determine that members of the information technology and operations groups conducted a new customer welcome call with new customers to review requested settings to help ensure that the services to be provisioned matched the customer's expectations.	No exceptions noted.
		Inspected evidence of new customer welcome calls for a sample of customers provisioned during the review period to determine that members of the information technology and operations groups conducted a new customer welcome call for 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, company intranet site, and 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.
CC2.3.5	A completed engineering document and client contact form is required prior to the provisioning process that include, but is not limited to, the following: • Contact information • Network connectivity requirements • Network redundancy requirements • Customer cabinet layout	Inquired of the director, IT compliance regarding customer implementations to determine that a completed engineering document and client contact form was obtained prior to the provisioning process 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 review 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
CC2.3.6	A dedicated NOC is staffed 24 hours per day to respond to customer inquiries, support issues, and incidents.	Inspected the NOC staffing schedules for a sample of weeks during the review 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 configurations and example incident ticket resolved during the review period to determine that operations personnel utilized a ticketing system to track the status of incidents and service disruptions.	No exceptions noted.
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 • Priority • Problem type • Description of event • Correspondence with customers • Resolution details	**Inspected a sample of incident tickets recorded during the review period to determine that each ticket sampled included the following:** • **Date and time of the incident** • **Priority** • **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 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.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.1.3	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 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 review period.	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 EVP of security and director of IT 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.
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 risk assessment was performed during the review period and that risks that were identified were rated using a risk evaluation process and were formally documented, along with mitigation strategies, for management review.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.2.4	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 EVP of security 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 during the review 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 or regulations are considered by senior management.	Inquired of the EVP of Security regarding emerging technologies and the applicable laws or regulations to determine that the entity's IT security group monitored the security impact of emerging technologies, and the impact of applicable laws or regulations were considered by senior management.	No exceptions noted.
		Inspected example security update e-mail notification received during the review period to determine that the entity's IT security group monitored the security impact of emerging technologies.	No exceptions noted.
CC3.3 COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
CC3.3.1	Management performs a risk assessment on an annual basis that includes consideration of the potential for fraud.	Inquired of the director of IT regarding the risk compliance process to determine that management performed a risk assessment during the review period that includes consideration of the potential for fraud.	No exceptions noted.
		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 review period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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 EVP of security 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 during the review 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 or regulations are considered by senior management.	Inquired of the EVP of Security regarding emerging technologies and the applicable laws or regulations to determine that the entity's IT security group monitored the security impact of emerging technologies, and the impact of applicable laws or regulations were considered by senior management.	No exceptions noted.
		Inspected example security update e-mail notification received during the review period to determine that the entity's IT security group monitored the security impact of emerging technologies.	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	A vulnerability scan is performed by a third-party vendor on an annual basis to identify threats and assess their potential impact to the systems. Results are included in the risk assessment and remediations are monitored through resolution.	Inspected the most recent vulnerability scan results to determine that a vulnerability scan was performed by a third-party vendor during the review period to identify threats and assess their potential impact to the systems and results were included in the risk assessment and remediations were monitored through resolution.	No exceptions noted.
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 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.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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.	Inspected the most recent internal audit report to determine that internal audits were performed during the review period to help ensure that internal controls are designed and operating effectively to achieve organizational objectives and the results of audits were reviewed by management to develop and implement corrective action plans for control weaknesses as needed.	No exceptions noted.
CC4.1.4	The board of directors' reviews internal control performance metrics provided by management on an annual basis.	Inspected the most recent board of directors meeting minutes to determine that the board of directors reviewed internal control performance metrics provided by management during the review 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	A vulnerability scan is performed by a third-party vendor on an annual basis to identify threats and assess their potential impact to the systems. Results are included in the risk assessment and remediations are monitored through resolution.	Inspected the most recent vulnerability scan results to determine that a vulnerability scan was performed by a third-party vendor during the review period to identify threats and assess their potential impact to the systems and results were included in the risk assessment and remediations were monitored through resolution.	No exceptions noted.
CC4.2.2	Internal audits are performed on an annual basis to 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.	Inspected the most recent internal audit report to determine that internal audits were performed on an annual basis to ensure that internal controls are designed and operating effectively to achieve organizational objectives and the results of audits were reviewed by management to develop and implement corrective action plans for control weaknesses as needed.	No exceptions noted.
CC4.2.3	The board of directors' reviews internal control performance metrics provided by management on an annual basis.	Inspected the most recent board of directors meeting minutes to determine that the board of directors reviewed internal control performance metrics provided by management during the review period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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 risk assessment was performed during the review period and that risks that were identified were rated using a risk evaluation process and were formally documented, along with mitigation strategies, for management review.	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 privileges and zone definitions to determine that badge access card privileges were assigned to users using predefined access zones to help ensure that access privileges were consistently assigned based on job responsibilities and/or where customer equipment was located.	No exceptions noted.
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 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 man-trap 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 in-scope data centers entrance process to determine that personnel and authorized customers and contractors were required to enter a man-trap 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.	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 access within the in-scope data centers 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.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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 EVP of security 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.	No exceptions noted.
CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC5.3.1	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 and company intranet site 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 identifies 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.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.3.4	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.	Inspected the employee handbook acknowledgment form for a sample of employees hired during the review period to determine that policies and procedures required that employees signed an acknowledgment form 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 for each employee sampled.	No exceptions noted.
CC5.3.5	An employee sanction policy is in place that address 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 address remedial actions for lack of compliance with policies and procedures.	No exceptions noted.
Logical and Physical Access Controls			
CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
CC6.1.1	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 EVP of security and director of IT 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 identifies 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
CC6.1.3	Access to the network domain requires the use of a unique username and password.	Inspected the network domain user access privileges 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 access privileges 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.
CC6.1.5	Access to the operating system requires the use of a unique username and password.	Inspected the operating system user access privileges and authentication configurations for a sample of production servers to determine that access to the operating system for each production 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 for the operating system access for each production server sampled were derived from the corporate network domain controller.	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 access privileges and authentication screen 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 screen to determine that authentication parameters for the badge access system were derived from the corporate network domain controller.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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 required 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 authentication 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.
CC6.1.12	Authentication parameters for the centralized authentication system are derived from the corporate network domain controller.	Inspected the centralized authentication system authentication 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 administrative access privileges 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 administrative access privileges for a sample of production servers to determine that administrative access privileges within the operations system for each production server sampled were restricted to user accounts accessible by authorized personnel.	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 user access privileges to determine that the ability to create, modify, or delete user badge access privileges to the facilities was restricted to user accounts accessible by persons authorized personnel.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.1.16	Administrative access privileges within the VPN system are restricted to user accounts accessible by authorized personnel.	Inspected the VPN system administrative access privileges 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 to determine that the ability to access and administer network infrastructure was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
CC6.1.18	Predefined security groups are utilized to assign role-based access privileges and segregate access to data to the network domain.	Inspected the network domain user access privileges and role assignments to determine that predefined security groups were utilized to assign role-based access privileges and segregate 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 segregate access to data to the operating system.	Inspected the operating system user access privileges and role assignments for a sample of production servers to determine that predefined security groups were utilized to assign role-based access privileges and segregate access to data to the operating system for each production server sampled.	No exceptions noted.
CC6.1.20	Predefined security groups are utilized to assign role-based access privileges and segregate access to data to the badge access system.	Inspected the badge access system user access privileges and role assignments to determine that predefined security groups were utilized to assign role-based access privileges and segregate 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 segregate access to data to the centralized authentication system.	Inspected the centralized authentication system user access privileges and role assignments to determine that predefined security groups were utilized to assign role-based access privileges and segregate access to data to the centralized authentication system.	No exceptions noted.
CC.6.1.22	Predefined security groups are utilized to assign role-based access privileges and segregate access to data to the VPN system.	Inspected the VPN system user access privileges and role assignments to determine that predefined security groups were utilized to assign role-based access privileges and segregate access to data to the VPN system.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.1.23	A firewall system is in place to filter unauthorized inbound network traffic from the Internet.	Inspected the firewall system rulesets for a sample of in-scope firewalls to determine that each firewall system sampled was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
CC6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			
CC6.2.1	Department managers complete a new hire onboarding checklist prior to the granting of 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 completed a new hire onboarding checklist to the granting of system access privileges to new employees.	No exceptions noted.
		Inspected the new hire onboarding checklists for a sample of employees hired during the review 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 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 recently completed semi-annual user access review to determine that a full review of employee and customer access privileges was performed during the review period.	No exceptions noted.
CC6.2.3	A completed engineering document and client contact form is required prior to the provisioning process that include, but is not limited to, the following: • Contact information • Network connectivity requirements • Network redundancy requirements • Customer cabinet layout	Inquired of the director of network engineering operations regarding customer implementations to determine that a completed engineering document and client contact form was obtained prior to the provisioning process included the following: • Contact information • Network connectivity requirements • Network redundancy requirements • Customer cabinet layout	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the completed provisioning questionnaire for a sample of customers provisioned during the review period to determine that a completed provisioning questionnaire was obtained for each customer sampled.	No exceptions noted.
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 checklists for a sample of employees terminated during the review period to determine that a termination checklist was completed as a component of the employee termination process for each terminated employee sampled.	No exceptions noted.
		Inspected the systems access privileges for a sample of employees terminated during the review period to determine that systems access rights were revoked for each terminated 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 the granting of 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 completed a new hire onboarding checklist to the granting of system access privileges to new employees.	No exceptions noted.
		Inspected the new hire onboarding checklists for a sample of employees hired during the review 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 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 recently completed semi-annual user access review to determine that a full review of employee and customer access privileges was performed during the review 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 include, but is not limited to, the following: • **Contact information** • **Network connectivity requirements** • **Network redundancy requirements** • **Customer cabinet layout**	**Inquired of the director of network engineering operations regarding customer implementations to determine that a completed engineering document and client contact form was obtained prior to the provisioning process 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 review 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 checklists for a sample of employees terminated during the reporting period to determine that a termination checklist was completed as a component of the employee termination process for each terminated employee sampled.	No exceptions noted.
		Inspected the systems access privileges for a sample of employees terminated during the review period to determine that systems access rights were revoked for each terminated 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 administrative access privileges 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 administrative access privileges for a sample of production servers to determine that administrative access privileges within the operations system for each production server sampled were 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
CC6.3.7	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 user access privileges to determine that the ability to create, modify, or delete user badge access privileges to the facilities was restricted to user accounts accessible by persons 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 administrative access privileges 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 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 segregate access to data to the network domain.	Inspected the network domain user access privileges and role assignments to determine that predefined security groups were utilized to assign role-based access privileges and segregate 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 segregate access to data to the operating system.	Inspected the operating system user access privileges and role assignments for a sample of production servers to determine that predefined security groups were utilized to assign role-based access privileges and segregate access to data to the operating system for each production server sampled.	No exceptions noted.
CC6.3.12	Predefined security groups are utilized to assign role-based access privileges and segregate access to data to the badge access system.	Inspected the badge access system user access privileges and role assignments to determine that predefined security groups were utilized to assign role-based access privileges and segregate access to data to the badge access system.	No exceptions noted.
CC6.3.13	Predefined security groups are utilized to assign role-based access privileges and segregate access to data to the centralized authentication system.	Inspected the centralized authentication system user access privileges and role assignments to determine that predefined security groups were utilized to assign role-based access privileges and segregate access to data to the centralized authentication system.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.3.14	Predefined security groups are utilized to assign role-based access privileges and segregate access to data to the VPN system.	Inspected the VPN system user access privileges and role assignments to determine that predefined security groups were utilized to assign role-based access privileges and segregate 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 and addressed 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 user access privileges to determine that the ability to create, modify, or delete user badge access privileges to the facilities was restricted to user accounts accessible by persons 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 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 recently completed semi-annual user access review to determine that a full review of employee and customer access privileges was performed during the review period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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 privileges and zone definitions to determine that badge access card privileges were assigned to users using predefined access zones to help 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 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 badge access privileges for a sample of employees terminated during the review period to determine that badge access privileges were revoked for each terminated 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 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 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.
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 director of IT compliance regarding the visitor sign-in process to determine that visitors were required to 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 to determine that visitors were required to present a picture identification card, which was either retained or digitally scanned, and were escorted during the sign-in process.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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 director of IT compliance regarding access within the facilities to determine that personnel at the facilities were distinguished as being one of the following: • **Employees with badge access cards** • **Customers with badge access cards** • **Contractors with badge access cards** • **Visitors with non-functioning visitor badges**	**No exceptions noted.**
		Observed personnel within the facilities to determine that personnel were distinguished by the following badge access card designations: • **Employees – red colored badge access cards and lanyards – Security has red-colored badges but wear 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.**
CC6.4.12	Personnel and authorized customers and contractors are required to enter a man-trap 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 to determine that employees and authorized customers and contractors were required to enter a man-trap where they provided the 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 access within the data centers to determine that badge access and biometric identification were required for ingress and egress to the interior doors of the data centers.	No exceptions noted.
CC6.4.14	Visitors without badge access cards are required to be escorted by authorized employees while within the facilities.	Observed visitor access procedures to determine that visitors without badge access cards were escorted while within the facilities.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the access control policy to determine that visitors were required 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 director of IT 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 a sample of activity logs recorded during the review period to determine that the following attributes for physical movements within the facilities were captured and maintained during the review period: • Date/time • Event • Badge access card details • Device	No exceptions noted.
CC6.4.16	Digital surveillance video cameras record activities at facility entrances, the building perimeters, and other areas within the facilities.	Observed the security command center 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 in-scope data centers 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 the facilities entrances and manage visitor access 24 hours per day.	Observed the security personnel at the security command center to determine that security personnel monitored access to the facilities and managed visitor access.	No exceptions noted.
		Inspected the master shift schedule for security personnel to determine that security personnel were staffed to monitor access to the facilities on a 24 hour per day basis during the review period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.4.20	Security personnel utilize an incident reporting system to document any physical security incidents.	Inspected a recent incident report to determine that security personnel utilized an incident reporting system to document any physical security incidents during the review 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 to determine that the physical security hardware was secured behind locked server racks and physical cages.	No exceptions noted.
CC6.4.22	Physical access to the data center is documented and approved by the employee's manager prior to granting of access.	Inspected the physical access request approvals for a sample of employees and contractors granted access during the review period to determine that physical access to the data center was documented and approved by the employee's manager prior to granting of access for each employee and contractor sampled.	No exceptions noted.
CC6.4.23	Physical access to the customer cages is documented and approved by the customer prior to granting of access.	Inspected the physical access request approvals to the customer cages for a sample of vendors and customers granted access during the review period to determine that physical access to the customer cages was documented and approved by the customer prior to granting of access 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.
CC6.6 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 rulesets for a sample of in-scope firewalls to determine that each firewall system sampled was in place 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
CC6.6.2	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 applications' configurations and example e-mail alert notifications generated during the review 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.
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 help 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 required for remote access to production and enforced two-factor authentication.	No exceptions noted.
CC6.6.5	A vulnerability scan is performed by a third-party vendor on an annual basis to identify threats and assess their potential impact to the systems. Results are included in the risk assessment and remediations are monitored through resolution.	Inspected the most recent vulnerability scan results to determine that a vulnerability scan was performed by a third-party vendor during the review period to identify threats and assess their potential impact to the systems and results were included in the risk assessment and remediations were monitored through resolution.	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 required 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 help 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 data transmission 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 every 60 minutes • 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 every 60 minutes • 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	A vulnerability scan is performed by a third-party vendor on an annual basis to identify threats and assess their potential impact to the systems. Results are included in the risk assessment and remediations are monitored through resolution.	Inspected the most recent vulnerability scan results to determine that a vulnerability scan was performed by a third-party vendor during the review period to identify threats and assess their potential impact to the systems and results were included in the risk assessment and remediations were monitored through resolution.	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 logging and monitoring process to determine that IT personnel reviewed network domain event logs on an ad hoc basis during the review period.	No exceptions noted.
		Inspected the network domain logging configurations and an example network domain event log generated during the review 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 logging and monitoring process to determine that IT personnel reviewed operating system event logs during the review period.	No exceptions noted.
		Inspected the operating system logging configurations for a sample of production servers and an example operating system event log generated during the review period to determine that each production server operating system sampled was configured to log the following events: • Account logon events • Account management events • Logon events • Policy changes	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.1.4	Activity logs of certain physical movements within the facilities are monitored and maintained.	Inquired of the director of IT 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 a sample of activity logs recorded during the review period to determine that the following attributes for physical movements within the facilities were captured and maintained during the review 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 review period.	No exceptions noted.
		Inspected the firewall system logging configurations for a sample of in-scope firewall systems during the review period to determine that each firewall system sampled was configured to log activity that included the following information: • 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 review period.	No exceptions noted.
		Inspected the VPN system logging configurations and an example VPN system event log generated during the review period to determine that the VPN system was configured to log activity that included the following information: • Failed login attempts • Successful login attempts	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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 review period.**	**No exceptions noted.**
		Inspected the centralized authentication system logging configurations and example logs generated during the review 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 applications' configurations and example e-mail alert notifications generated during the review 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 director of IT compliance 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 a sample of activity logs recorded during the review period to determine that the following attributes for physical movements within the facilities were captured and maintained during the reporting 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
CC7.2.2	Digital surveillance video cameras record activities at facility entrances, the building perimeters, and other areas within the facilities.	Observed the security command center 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 data centers 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 the facilities entrances and manage visitor access 24 hours per day.	Observed the security personnel at the security command center to determine that security personnel monitored access to the facilities and managed visitor access.	No exceptions noted.
		Inspected the master shift schedule for security personnel to determine that security personnel were staffed to monitor access to the facilities on a 24 hour per day basis during the review period.	No exceptions noted.
CC7.2.6	Security personnel utilize an incident reporting system to document any physical security incidents.	Inspected a recent incident report to determine that security personnel utilized an incident reporting system to document any physical security incidents during the review period.	No exceptions noted.
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 director of IT regarding the monitoring of temperature and humidity levels to determine that operations personnel monitored temperature and humidity levels and that identified issues were responded to as necessary.	No exceptions noted.
		Inspected the monitoring system configurations 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
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 e-mail notification generated during the review 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, company intranet site, and 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.	Inspected the NOC staffing schedules for a sample of weeks during the reporting 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 history and an example ticket resolved during the review period to determine that IT personnel utilized an automated ticketing system to document security violations, responses, and resolution.	No exceptions noted.
CC7.3.4	Management meetings are held on a weekly basis to discuss incidents and corrective measures to help ensure that incidents are resolved.	Inquired of the director of IT regarding management meetings to determine that management meetings were held on a weekly basis to discuss incidents and corrective measures to help ensure that incidents were resolved.	No exceptions noted.
		Inspected the management meeting minutes for a sample of weeks during the review period to determine that management meetings were held to discuss incidents and corrective measures for each week sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.3.5	Change management meetings are held on a weekly basis to discuss and communicate the ongoing and upcoming projects that affect the system.	Inquired of the director of IT compliance regarding change management meetings to determine that change management meetings were held on a weekly basis to discuss and communicate the ongoing and upcoming projects that affected the system.	No exceptions noted.
		Inspected the recurring calendar meeting invitation, agenda, and minutes for a sample of weeks during the review period to determine that change management meetings were held to discuss and communicate the ongoing and upcoming projects that affect the system 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, company intranet site, and 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 history and an example ticket resolved during the review period to determine that IT personnel utilized an automated ticketing system to document security violations, responses, and resolution.	No exceptions noted.
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, company intranet site, and 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
CC7.5.2	Management meetings are held on a weekly basis to discuss incidents and corrective measures to help ensure that incidents are resolved.	Inquired of the director of IT regarding management meetings to determine that management meetings were held on a weekly basis to discuss incidents and corrective measures to help ensure that incidents were resolved.	No exceptions noted.
		Inspected the management meeting minutes for a sample of weeks during the review 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.
CC8.1.2	Automated ticketing systems are utilized to log and track in-scope system infrastructure change information, impacted system resources, and management approvals.	Inspected the ticketing systems for a sample of infrastructure changes implemented during the review period to determine that automated ticketing systems were utilized to log and track in-scope system infrastructure change information, impacted system resources, and management approvals for each change sampled.	No exceptions noted.
CC8.1.3	Change management meetings are held on a weekly basis to discuss and communicate the ongoing and upcoming projects that affect the system.	Inquired of the director of IT compliance regarding change management meetings to determine that change management meetings were held on a weekly basis to discuss and communicate the ongoing and upcoming projects that affected the system.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the recurring calendar meeting invitation, agenda, and minutes for a sample of weeks during the review period to determine that change management meetings were held to discuss and communicate the ongoing and upcoming projects that affect the system for each week 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 review 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 user access privileges to determine that the ability to implement infrastructure changes was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
CC8.1.6	IT personnel utilize an automated ticketing system to document security violations, responses, and resolution.	Inspected the ticketing system history and an example ticket resolved during the review period to determine that IT personnel utilized an automated ticketing system to document security violations, responses, and resolution.	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.	No exceptions noted.
CC9.2 The entity assesses and manages risks associated with vendors and business partners.			
CC9.2.1	Documented vendor management policy is 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 policy to determine that documented vendor management policy was 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 the 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 review period.	No exceptions noted.
CC9.2.3	Management performs due diligence prior to onboarding a vendor or business partner to ensure third parties are in compliance with the organization's security and availability commitments.	Inspected examples of vendor risk assessments to determine that management performed due diligence prior to onboarding a vendor or business partner to ensure third parties were in compliance with the organization's security and availability commitments.	No exceptions noted.
CC9.2.4	Management reviews vendor audit reports on an annual basis to ensure that vendors or business partners are in compliance with the organization's security and availability commitments.	Inspected examples of vendor reviews to determine that management reviewed vendor audit reports to ensure that vendors or business partners were in compliance with the organization's security and availability commitments during the review 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 applications' configurations and example e-mail alert notifications generated during the review 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	A dedicated NOC is staffed 24 hours per day to respond to customer inquiries, support issues, and incidents.	Inspected the NOC staffing schedules for a sample of weeks during the review period to determine that the NOC was staffed 24 hours per day for each week sampled.	No exceptions noted.
A1.1.3	Management meetings are held on a weekly basis to discuss incidents and corrective measures to help ensure that incidents are resolved.	Inquired of the director of IT regarding management meetings to determine that management meetings were held on a weekly basis to discuss incidents and corrective measures to help ensure that incidents were resolved.	No exceptions noted.
		Inspected the management meeting minutes for a sample of weeks during the review 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 centers are equipped with the following environmental protection equipment: • Fire detection and suppression equipment • UPS systems • Generators • Air conditioning units	Observed the environmental protection equipment within the in-scope data centers to determine that the data centers were equipped with the following environmental protection equipment: • Fire detection and suppression equipment • UPS systems • Generators • Air conditioning units	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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 systems inspection reports for a sample of quarters during the review period to determine that the business process director obtained inspection reports as evidence that the fire suppression systems underwent maintenance inspections for each quarter sampled.	No exceptions noted.
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 systems inspection reports for a sample of quarters during the review period to determine that the business process director obtained inspection reports as evidence that the fire alarm systems underwent maintenance inspections for each quarter sampled.	No exceptions noted.
A1.2.4	The Director of Maintenance Administration obtains inspection tags as evidence that the hand-held fire extinguishers undergo maintenance inspections on an annual basis.	Observed the current inspection tags for a sample of hand-held fire extinguishers for in-scope data centers to determine that the Director of Maintenance Administration obtained inspection tags as evidence that each hand-held fire extinguisher sampled underwent maintenance inspections during the review 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 systems inspection reports for a sample of quarters during the review period to determine that the business process director obtained inspection reports as evidence 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 systems inspection reports for a sample of quarters during the review period 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 reports for a sample of quarters during the review period to determine that the business process director obtained inspection reports as evidence that the generators 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
A1.2.8	Internal personnel perform preventative maintenance procedures on the generators on at a monthly basis.	Inspected the generator inspection reports for a sample of months during the review period to determine that internal personnel performed preventative maintenance procedures on the generators for each month sampled.	No exceptions noted.
A1.2.9	The business process director obtains inspection reports as evidence that the UPS systems undergo maintenance inspections on an annual basis.	Inspected the most recent UPS systems inspection reports to determine that the business process director obtained inspection reports as evidence that the UPS systems underwent maintenance inspections during the review period.	No exceptions noted.
A1.2.10	Internal personnel perform preventative maintenance procedures on the UPS systems on a semi-annual basis.	Inspected the most recent semi-annual UPS systems inspection reports to determine that internal personnel performed preventative maintenance procedures on the UPS systems during the review period.	No exceptions noted.
A1.2.11	A dedicated NOC is staffed 24 hours per day to respond to customer inquiries, support issues, and incidents.	Inspected the NOC staffing schedules for a sample of weeks during the review period to determine that the NOC was staffed 24 hours per day for each week sampled.	No exceptions noted.
A1.2.12	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.
A1.2.13	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.
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 review 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 our energy from renewable sources is a central part of our 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
http://awea.files.cms-plus.com/FileDownloads/pdfs/Nevada.pdf

SOC 1 REPORT

FOR

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, 2021, TO SEPTEMBER 30, 2022

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 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 Colocation Services system throughout the period October 1, 2021, to September 30, 2022 (the "description"), and the suitability of the design and operating effectiveness of controls included in the description to achieve the related control objectives stated in the description, based on criteria identified in "Management's Assertion" in Section 2 (the "assertion"). The controls and control objectives included in the description are those that management of 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 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.

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. 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, 2021, to September 30, 2022. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- Performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on the criteria in management's assertion;
- Assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description;

- Testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved; and
- Evaluating the overall presentation of the description, suitability of the control objectives stated in the description, and suitability of the criteria specified by the service organization in its assertion.

Service Auditor's Independence and Quality Control

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

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in processing or reporting transactions in providing the 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 Colocation Services system that was designed and implemented throughout the period October 1, 2021, to September 30, 2022;

b. the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period October 1, 2021, to September 30, 2022, 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, 2021, to September 30, 2022; 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, 2021, to September 30, 2022, 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, 2021, to September 30, 2022.

Restricted Use

This report, including the description of the tests of controls and results thereof in the Testing Matrices, is intended solely for the information and use of management of Switch, user entities of Switch's Colocation Services system during some or all of the period October 1, 2021, to September 30, 2022, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatement of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than the specified parties.

Schellman & Company, LLC

Tampa, Florida
November 2, 2022

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, 2021, to September 30, 2022 (the "description"), for user entities of the system during some or all of the period October 1, 2021, to September 30, 2022, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities 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 Colocation Services system made available to user entities of the system during some or all of the period October 1, 2021, to September 30, 2022, for providing 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 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 Colocation Services system during the period covered by the description; and

   iii. does not omit or distort information relevant to the scope of the 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

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, 2021, to September 30, 2022, 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, 2021, to September 30, 2022. The criteria we used in making this assertion were that:

   i. the risks that threaten the achievement of the control objectives stated in the description have been identified by management of 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 all 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 virtually unlimited 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 rich technology ecosystem that benefits its participants. Switch continues to further enhance these benefits as they innovate and expand their platform ecosystem. Switch currently has more than 980 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 thirteen colocation facilities with an aggregate of over 4.8 million gross square feet (GSF) of space. These facilities have up over 500 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 our advanced colocation facilities while reducing exposure to the 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 our enterprise customers.

As additional locations and sectors within our 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 considerable. 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 man-trap relay logic. Each mantrap includes fixed cameras viewing every door.

Every 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 every person 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 HD with automatic low-light switching, capable of viewing up to .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. IOU provides a better use of the system to include constant monitoring, use of the 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 state-of-the-art environmental controls to protect the systems of its customers as well as operating in the most energy-efficient means possible. 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, capable and 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 Las Vegas 2, Las Vegas 4, Las Vegas 5, Las Vegas 7, Las Vegas 8, Las Vegas 9, Las Vegas 10, Las Vegas 11, Las Vegas 12, and Las Vegas 15 facilities located in Las Vegas, Nevada, as well as, the single Colocation Services facilities located in Reno, Nevada, Grand Rapids, Michigan, and Atlanta, Georgia. 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 document.

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, operating system platforms and databases, as shown in the table below:

Primary Infrastructure			
Production Application	**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.	Microsoft 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.	Microsoft 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 both the Honeywell MAXPRO Video Management System (VMS) and Milestone 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, these 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 Las Vegas 15 (LAS 15) data center facility was operational as of March 29, 2022. The test of controls at the facility only apply to the facility's dates of operation during the specified reporting period of March 29, 2022, to September 30, 2022, for the Las Vegas 15 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 Directors and Operations Management.

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of 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 include:

- 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 Directors and Audit Committee Oversight

Switch's control consciousness is influenced significantly by its Owners and Board of Directors' participation. A Board of Directors 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 appropriate 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 appropriate 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 appropriate 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 services provided.
- Management meetings are held on a periodic basis to discuss operational issues.

Switch's human resources 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 on-boarding 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 acknowledgement of receipt of employee handbook document; and
    - Verification that the employee has taken security training and signed an acknowledgement 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 the management's description of the services organizations systems. 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 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 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 are 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 Directors 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 code of conduct, entity values and behavioral standards. Employees are required to sign an acknowledgement form 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 requires employees to complete a training program to help ensure that employees have the necessary training to carry out their responsibility.

Human Resource Management

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

Switch has documented policies and procedure for employee on-boarding and off-boarding. 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 acknowledgement 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 for 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 (i.e., 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. Pre-defined access groups are utilized to provide access depending on the individual's role and responsibilities. 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. 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 ad-hoc 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 ad-

hoc review. The facilities are monitored 24 hours per day by security personal with the use of motion sensitive digital surveillance cameras, alarms, and motion detectors. 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 information technology 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.

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 pre-defined thresholds are exceeded.

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. Utility power is run through the UPS battery systems so that customers are always receiving 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 is always drawing power from the UPS battery systems, ensuring smooth transitions from utility to generator and back again. On an annual basis, a third-party specialist inspects the UPS systems and generators to help ensure that the systems are in proper working order. 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. 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: Controls 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 pre-defined 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 will verify the request was initiated by an authorized customer contact. In the event that the request was initiated by an unauthorized customer, NOC personnel will 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 will be 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 will then schedule a new customer welcome call. During this call the members of the IT and operations groups will go over the customer cage or cabinet set up and provide the customer with and the 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
- AT&T
- ATT Michigan (Michigan Bell Telephone Company)
- Bandwidth Infrastructure Group (BIG)
- Casair
- CC Communications
- Charter
- Cogent
- Comcast
- Cox
- Crown Castle (former Wilcon)
- Everstream (former Comlink)
- GTT
- IX Reach
- Lumen
- Masergy
- Megaport
- Packet Fabric
- Parker Fiber
- PCCW
- Roberts
- Sky Fiber
- Tata
- Telepacific
- Time Warner Cable
- T-Mobile (former 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 the company'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.

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 make 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 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 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, 2021, through September 30, 2022.

Tests of Operating Effectiveness

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

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

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

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

Sampling

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

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

Test Results

The results of each test applied are listed alongside each respective test applied within the Testing Matrices. Test results not deemed as control deviations are noted by the phrase "No exceptions noted." in the test result column of the Testing Matrices. Any phrase other than the aforementioned constitutes a test result that is the result of a change in the application of the control activity, 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, 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 appropriate 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 communicated entity values and behavioral standards to personnel.	No exceptions noted.
1.03	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.	Inspected the employee handbook acknowledgment form for a sample of employees hired during the period to determine that policies and procedures require that employees sign an acknowledgement form 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 for each employee sampled.	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 to determine that employees had adequate training material to carry out their job responsibilities.	No exceptions noted.
1.05	A Board of Directors is in place to oversee management activities.	Inquired of management regarding the Board of Directors to determine that a Board of Directors was in place to oversee management activities.	No exceptions noted.
		Observed the meeting minutes for a sample of Board of Directors' meetings held during the period to determine that a Board of Directors was in place and met during the period.	No exceptions noted.

HUMAN RESOURCES MANAGEMENT

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that employee onboarding and off-boarding 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 evidence of 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 evidence of completed drug screening tests 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 agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.	Inspected the signed confidentiality statements for a sample of employees hired during the period to determine that each employee sampled signed a confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.	No exceptions noted.
2.04	Employees, customers, and vendors must undergo orientation 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, customer, and vendors must undergo orientation to help 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 orientation included the following: • **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 orientation acknowledgements with respect to the information security policy for a sample of employees hired during the period to determine that each employee sampled acknowledged their responsibilities with respect to information security.	No exceptions noted.
		Inspected the arc flash safety procedures and evidence of completed training for a sample of employees hired during the period to determine that each employee sampled completed electrical system safety training.	No exceptions noted.
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 badge access and system privileges for a sample of employees terminated during the period to determine that access and system privileges to systems were revoked for each terminated 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.
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 and addressed 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 user 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 persons 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.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the results of the most recently completed semi-annual user access review to determine that a full review of employee and customer access privileges was performed during 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 privileges and zone definitions to determine that badge access card privileges were assigned to users using predefined access zones to help ensure that access privileges were consistently assigned based on job responsibilities and/or where customer equipment was located.	No exceptions noted.
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 badge access privileges for a sample of employees terminated during the period to determine that badge access privileges were revoked for each terminated employee sampled.	No exceptions noted.
	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 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 Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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 Security Operations regarding the visitor sign-in process to determine that visitors were required to 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 to determine that visitors were required to present a picture identification card, which was either retained or digitally scanned, and were escorted 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 granting of access.	Inspected the physical access request approvals 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 granting of access 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 Security Operations regarding access within the in-scope facilities to determine that personnel at the facilities were distinguished as being one of the following: • Employees with badge access cards • Customers with badge access cards • Contractors with badge access cards • Visitors with non-functioning visitor badges	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 has red-colored badges but wear 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 in-scope data centers entrance process to determine that personnel and authorized customers and contractors were 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.	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 access within the in-scope data centers 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 visitor access procedures to determine that visitors without badge access cards were escorted while within the facilities.	No exceptions noted.
		Inspected the access control policy to determine that visitors were required to be 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
3.16	Physical access to the customer cages is documented and approved by the customer prior to granting of access.	Inspected the physical access request approvals to the 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 granting of access 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 Security Operations 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 a sample of 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 security command center to determine that digital surveillance video cameras recorded activities at facility entrances, the building perimeters, and other areas within the facilities.	No exceptions noted.
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.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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 in-scope data centers 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 the facilities entrances and manage visitor access 24 hours per day.	Observed the security personnel at the security command center to determine that security personnel monitored access to the facilities and managed visitor access.	No exceptions noted.
		Inspected the master shift schedule for security personnel 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 any physical security incidents.	Inspected a recent incident report to determine that security personnel utilized an incident reporting system to document any 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 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 information technology 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 formal 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 in-scope data center 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 Operations regarding fire suppression to determine that the dual-interlock (pre-action) dry pipe water sprinklers required both a smoke detection event and the activation of sprinklers to release water into the pipes.	No exceptions noted.
		Observed the in-scope data center facilities to determine that the data centers were equipped with pre-action water sprinklers.	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 systems inspection reports for a sample of quarters during the period to determine that the business process director obtained inspection reports as evidence 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 systems inspection reports for a sample of quarters during the period to determine that the business process director obtained inspection reports as evidence 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 current inspection tags for a sample of hand-held fire extinguishers to determine that the business process director obtained inspection tags as evidence 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 guided 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 Security Operations regarding the monitoring of temperature and humidity levels to determine that operations personnel monitored temperature and humidity levels and that identified issues were responded to, as necessary.	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 notifications generated during the period 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 within the in-scope data centers to determine that the data centers utilized redundant air conditioning units.	No exceptions noted.
		Observed the server farm layout to determine that 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 to determine that the devices were 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 systems inspection reports for a sample of quarters during the period to determine that the business process director obtained inspection reports as evidence 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 systems inspection reports for a sample of quarters during the period 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 for in-scope data centers 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 presence of the UPS systems for in-scope data centers 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 e-mail notification 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 reports for a sample of quarters during the period to determine that the business process director obtained inspection reports as evidence 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 at a quarterly basis.	Inspected the generator inspection reports for a sample of quarters during the period 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	The business process director obtains inspection reports as evidence that the UPS systems undergo maintenance inspections on an annual basis.	Inspected the most recent UPS systems inspection reports to determine that the business process director obtained inspection reports as evidence that the UPS systems underwent maintenance inspections during 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 • RNO 1 • GRR 1 • ATL 1	**No exceptions noted.**
		Inspected the data center operations maintenance schedule and the go-live date of the LAS 15 data center facility with the assistance of the VP of Data Center Operations and determined that there were no UPS maintenance inspections required for LAS 15 during the period; therefore, no testing of operating effectiveness was performed.	

[Intentionally Blank]

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
4.18	Internal personnel perform preventative maintenance procedures on the UPS systems on a semi-annual basis.	Inspected the most recent semi-annual UPS systems inspection reports to determine that internal personnel performed preventative maintenance procedures on the UPS systems during 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 • RNO 1 • GRR 1 • ATL 1	**No exceptions noted.**
		Inspected the data center operations maintenance schedule and the go-live date of the LAS 15 data center facility with the assistance of the VP of Data Center Operations and determined that there were no UPS maintenance inspections required for LAS 15 during the period; therefore, no testing of operating effectiveness was performed.	
4.19	The data centers contain two distinct electrical connections to the electrical company's substation.	Inquired of the SVP of Security Operations regarding electric connectivity to determine that the data centers contained two distinct electrical connections to the electrical company's substation.	No exceptions noted.
		Observed the power connections to the facilities to determine that the facilities 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 pre-defined 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 pre-defined 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 help 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 authentication 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 authentication 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: Controls 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	Documenting 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 applications' configurations and an example e-mail alert notification 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 Director of IT Compliance 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 schedules 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 for each incident sampled operations personnel utilized a ticketing system to track the status of incidents and service disruptions.	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 for each incident sampled operations personnel recorded information regarding incidents and service disruptions in an incident ticket as a component of the customer support process and included the following:** • 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 operations personnel configure priority ratings for tickets created by the ticketing system 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 pre-defined 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 Director of IT Compliance 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 schedules 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.
7.04	Operations personnel utilize a ticketing system to track the status of incidents and service disruptions.	Inspected the ticketing system dashboard and example incident ticket resolved during the period to determine that operations personnel utilized a ticketing system to track the status of incidents and service disruptions.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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 a sample of incident tickets recorded during the period to determine that each ticket sampled included the following:** • 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 queries to determine that the ticketing system is configured for NOC personnel to perform real-time monitoring of open tickets that have 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 information technology and operations personnel in the customer provisioning process.	Inspected the customer provisioning policies and procedures and customer provisioning thank you template to determine that documented policies and procedures were in place to guide information technology and operations personnel in the customer provisioning process.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
8.02	Operations personnel require a customer service agreement to be executed in order to begin the implementation process.	Inspected the executed service agreements for a sample of customers provisioned during the period to determine that a customer service agreement was executed by operations personnel in order to begin 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 include, but is not limited to, the following: • Contact information • Network connectivity requirements • Network redundancy requirements • Customer cabinet layout	**Inquired of the Director of IT Compliance regarding customer implementations to determine that a completed engineering document and client contact form was obtained prior to the provisioning process 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.
8.04	Members of the information technology 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 customer implementations to determine that members of the information technology 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.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected evidence of new customer welcome calls for a sample of customers provisioned during the period to determine that members of the information technology and operations groups conducted a new customer welcome call with new customers to review requested settings to ensure that the services to be provisioned match the customer's expectations for each customer sampled.	No exceptions noted.

SWITCH, LTD.

INDEPENDENT SERVICE AUDITOR'S SOC 3 REPORT

FOR THE COLOCATION SERVICES

FOR THE PERIOD OF OCTOBER 1, 2021, TO SEPTEMBER 30, 2022

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, Ltd. Service Organization Management" ("assertion") that the controls within Switch's Colocation Services system ("system") were effective throughout the period October 1, 2021, to September 30, 2022, 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 (AICPA). 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; and
- 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, 2021, through September 30, 2022, 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 2, 2022

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, 2021, to September 30, 2022, 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, 2021, to September 30, 2022, 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, 2021, to September 30, 2022, 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 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 Chief Executive Officer (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 all 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 virtually unlimited 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 rich technology ecosystem that benefits its participants. Switch continues to further enhance these benefits as they innovate and expand their platform ecosystem. Switch currently has more than 980 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. We believe that traditional technology infrastructure is not capable of supporting the growing wave of mission critical data and increasingly powerful information technology (IT) equipment.

Switch presently owns and operates four primary campus locations, called Primes, which encompass thirteen colocation facilities with an aggregate of over 4.8 million gross square feet (GSF) of space. These facilities have over 500 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 our advanced colocation facilities while reducing exposure to the 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 our enterprise customers.

As additional locations and sectors within our 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 considerable. 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 every door.

Every 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 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 every person 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 HD with automatic low-light switching, capable of viewing up to .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. IOU provides a better use of the system to include constant monitoring, use of the 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 state-of-the-art environmental controls to protect the systems of its customers as well as operating in the most energy-efficient means possible. 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, capable and 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

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 Las Vegas 15 (LAS 15) data center facility was operational as of March 29, 2022. The test of the controls at the facility only apply to the facility's dates of operation during the specified reporting period of March 29, 2022, to September 30, 2022, for the Las Vegas 15 data center facility.

Principal Service Commitments and System Requirements

Switch designs business processes and procedures to meet its objectives for Colocation Services. Those objectives are based on the service commitments that Switch makes to user entities, the laws and regulations that govern the provision 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 security 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 confidentiality policies. Commitments and requirements of Switch are documented in customer contracts and are updated and signed upon any changes in the confidentiality practices.

In accordance with our 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

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

Primary Infrastructure			
Production Application	**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.	Microsoft 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.	Microsoft 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 both the Honeywell MAXPRO Video Management System (VMS) and the Milestone 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, these 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) department – 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.

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 will detail the specific production systems and required levels of access privileges. When an employee ends their employment, a termination checklist is completed to document the off-boarding 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 data center facilities. Pre-defined access groups are utilized to provide access depending on the individual's role and responsibilities. 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. 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 ad-hoc 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 ad-hoc review. The facilities are monitored 24 hours per day by security personal with the use of motion sensitive digital surveillance cameras, alarms, and motion detectors. 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.

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 pre-defined thresholds are exceeded.

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. Utility power is run through the UPS battery systems so that customers are always receiving 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 is always drawing power from the UPS battery systems, ensuring smooth transitions from utility to generator and back again. On an annual basis, a third-party specialist inspects the UPS systems and generators to help ensure that the systems are in proper working order. 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.

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.

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 network operations 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

Disaster recovery plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event. Disaster recovery tests are performed on an annual basis, and the results were recorded and tracked to identify potential threats.

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 manage, track, respond, and resolve network issues. 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.

Capacity and Availability Monitoring

SYSLOG is configured 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.

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 Colocation Services system.