CoreSite Realty Corporation

SOC 2 Report

For

Colocation Services

A Type 2 Independent Service Auditor's Report on
Controls Relevant to Security and Availability

July 1, 2016, to June 30, 2017

Attestation and Compliance Services

This report is intended solely for use by the management of CoreSite Realty Corporation, user entities of CoreSite Realty Corporation's services, and other parties who have sufficient knowledge and understanding of CoreSite Realty Corporation'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

INDEPENDENT SERVICE AUDITOR'S REPORT

To CoreSite Realty Corporation:

Scope

We have examined the attached description of CoreSite Realty Corporation's ("CoreSite" or the "service organization") colocation services for the period July 1, 2016, to June 30, 2017, (the "description") performed at the data center facilities listed in Section 3 of this report, based on the criteria set forth in paragraph 1.26 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* ("description criteria") and the suitability of the design and operating effectiveness of controls described therein to meet the criteria for the security and availability principles set forth in the 2016 TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Principles and Criteria)* ("applicable trust services criteria"), throughout the period July 1, 2016, to June 30, 2017.

Service organization's responsibilities

CoreSite has provided the attached assertion, in Section 2, about the fairness of the presentation of the description based on the description criteria and suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria. CoreSite is responsible for preparing the description of the service organization's system and the assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description of the service organization's system; selecting the trust services principle(s) addressed by the engagement and stating the applicable trust services criteria and related controls in the description of the service organization's system; identifying the risks that would prevent the applicable trust services criteria from being met; identifying any applicable trust services criteria related to the principle(s) being reported on that have been omitted from the description and explaining the reason for the omission; and designing, implementing, and documenting controls to meet the applicable trust services criteria.

Service auditor's responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description based on the description criteria and on the suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included procedures that we considered necessary in the circumstances. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is fairly presented based on the description criteria, and the controls were suitably designed and operating effectively to meet the applicable trust services criteria throughout the period July 1, 2016, to June 30, 2017.

Our examination involved performing procedures to obtain evidence about the fairness of the presentation of the description based on the description criteria and that the controls were suitably designed and operating effectively to meet the applicable trust services criteria throughout the period July 1, 2016, to June 30, 2017. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to meet the applicable trust services criteria. Our procedures also included testing the operating effectiveness of those controls to provide reasonable assurance that the applicable trust services criteria were met. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent limitations

Because of their nature and inherent limitations, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. Also, the projection to the future of any evaluation of the

fairness of the presentation of the description or conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable trust services criteria is subject to the risks that the system may change or that controls at a service organization may become inadequate or fail.

Emphasis of a Matter Paragraph

As indicated in CoreSite's description of its system, the SV7 data center facility was placed into service as of October 12, 2016. Therefore, any reference to controls at this facility is specific to the facility's dates of operation during the specified review period, October 12, 2016, to June 30, 2017, and we did not perform any tests of the design or operating effectiveness of controls related to SV7 data center facility outside of the period October 12, 2016, to June 30, 2017.

Opinion

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

a. the description fairly presents the system that was designed and implemented throughout the period July 1, 2016, to June 30, 2017;

b. the controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period July 1, 2016, to June 30, 2017; and

c. the controls that were tested, which were those necessary to provide reasonable assurance that the applicable trust services criteria were met, operated effectively throughout the period July 1, 2016, to June 30, 2017.

Description of test of controls

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

Restricted use

This report, including the description of tests of controls and results thereof in section 4 are intended solely for the information and use of CoreSite; user entities of CoreSite's colocation services system during some or all of the period July 1, 2016, to June 30, 2017; and prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization;
- How the service organization's system interacts with user entities, subservice organizations, or other parties;
- Internal control and its limitations;
- The nature of user entity controls responsibilities and their role in the user entities internal control as it relates to, and how they interact with, related controls at the service organization;
- The applicable trust services criteria; and
- The risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks.

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

Schellman & Company, LLC

Tampa, Florida
July 24, 2017

SECTION 2

MANAGEMENT'S ASSERTION

MANAGEMENT'S ASSERTION

We have prepared the attached description of CoreSite's colocation services for the period July 1, 2016, to June 30, 2017, (the "description") based on the criteria in items (a)(i)–(ii) below, which are the criteria for a description of a service organization's system in paragraph 1.26 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* (the "description criteria"). The description is intended to provide users with information about the colocation services system, particularly system controls intended to meet the criteria for the security and availability principles set forth in the 2016 TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Principles and Criteria)* ("applicable trust services criteria"). We confirm, to the best of our knowledge and belief, that

a. the description fairly presents the colocation services throughout the period July 1, 2016, to June 30, 2017, based on the following description criteria:

   i. The description contains the following information:

      1.) The types of services provided;

      2.) The components of the system used to provide the services, which are the following:

         a.) *Infrastructure*. The physical structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and telecommunications networks)

         b.) *Software*. The application programs and IT system software that supports application programs (operating systems, middleware, and utilities)

         c.) *People*. The personnel involved in the governance, operation and use of a system (developers, operators, entity users, vendor personnel, and managers)

         d.) *Procedures.* The automated and manual procedures

         e.) *Data*. Transaction streams, files, databases, tables, and output used or processed by a system;

      3.) The boundaries or aspects of the system covered by the description;

      4.) For information provided to, or received from, subservice organizations and other parties

         a.) How such information is provided or received and the role of the subservice organizations and other parties

         b.) The procedures the service organization performs to determine that such information and its processing, maintenance, and storage are subject to appropriate controls;

      5.) The applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, the following:

         a.) Complementary user entity controls contemplated in the design of the service organization's system

         b.) When the inclusive method is used to present a subservice organization, controls at the subservice organization;

      6.) If the service organization presents the subservice organization using the carve-out method

         a.) The nature of the services provided by the subservice organization

         b.) Each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the service organization, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria;

      7.) Any applicable trust services criteria that are not addressed by a control and the reasons; and

8.) In the case of a type 2 report, relevant details of changes to the service organization's system during the period covered by the description.

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

b. the controls stated in the description were suitably designed throughout the specified period to meet the applicable trust services criteria.

c. the controls stated in the description operated effectively throughout the specified period to meet the applicable trust services criteria.

As indicated in our description of the system, the SV7 data center facility was placed into service as of October 12, 2016. Therefore, any reference to controls at this facility is specific to the facility's dates of operation during the specified review period, October 12, 2016, to June 30, 2017.

SECTION 3

DESCRIPTION OF THE SYSTEM

OVERVIEW OF OPERATIONS

Company Background

CoreSite Realty Corporation (CoreSite) is engaged in the business of owning, acquiring, constructing, and managing technology-related real estate, and as of June 30, 2017, CoreSite's property portfolio included 20 operating data center facilities.

The company has built and managed data centers across the United States (US) since 2001, offering approximately 2.2 million net rentable square feet of data center space and colocation services to more than 1,200 customers.

Description of Services Provided

CoreSite provides facilities and infrastructure to protect customers' systems from physical and environmental security threats. Colocation services include, but are not limited to, physical security and access monitoring capabilities; climate controls and cooling systems; fire detection and suppression systems; and backup power infrastructure. A detailed description of each of the in-scope data center facilities is noted below.

BO1	
CoreSite's BO1 facility borders Cambridge and Boston's central business district, serving the many healthcare, financial, technological, and educational enterprises located in the area. BO1 is tethered to regional communication hubs and offers customers secure, reliable, high-performance solutions for their mission-critical business applications.	
Features / Size	253,000+ square feet of data center space Access to over 80 network, cloud, and information technology (IT) service providers Access to the CoreSite Open Cloud Exchange and Any2Exchange® for Internet peering, as well as leading cloud providers such as Amazon Web Services (AWS) Direct Connect
Deployments	Cabinets, cages, private suites, and build-to-suit Rooftop space available
Fit Out	Powered shell, infrastructure shell, and turn-key
Power	Alternating current (AC) and direct current (DC)
Uninterruptible Power Supply (UPS) / Power Distribution Unit (PDU) / Remote Power Panel (RPP) **Generators**	N, N+1, 2N redundancy N+1 redundancy
Certifications	Energy Star
Security	Key card access Biometric scanners Mantrap entry Perimeter and interior Internet protocol digital video recorder (IP-DVR) cameras 24x7x365 security by CoreSite security officers Controlled site access

MI1	
CoreSite's MI1 data center in Miami provides connectivity from the US to South America, as well as existing and scalable connectivity to the network access point (NAP) of the Americas. Built to withstand a Category 5 hurricane, MI1 is comprised of a diverse community of customers, including enterprises, domestic and international carriers, content delivery networks (CDNs), cloud computing, and IT service providers.	
Features / Size	43,000+ square feet of data center space Access to more than 30 natively deployed network and cloud providers, as well as tethered network communications hubs nearby Access to CoreSite's Any2Exchange® for Internet peering and Blended Internet protocol (IP)
Deployments	Cabinets, cages, private suites, and build-to-suit Rooftop space available
Fit Out	Powered shell, infrastructure shell, and turn-key
Power	AC and DC
UPS / PDU / RPP **Generators**	N, 2N redundancy N, N+1, 2N redundancy
Security	Key card access Biometric scanners Perimeter and interior IP-DVR cameras 24x7x365 security by CoreSite security officers 8' perimeter fence with controlled site access
NY1	
Located in the heart of Manhattan, NY1 stands at the epicenter of one of the most network dense markets in the world. Customers at CoreSite's NY1 facility have access to domestic and international carriers as well as leading cloud providers, including AWS Direct Connect. And, with direct dark fiber campus connectivity to CoreSite's NY2 facility in Secaucus, New Jersey, customers benefit from scalable data center deployments within the market.	
Features / Size	48,000+ square feet of data center space Access to the CoreSite Open Cloud Exchange, as well as leading cloud providers such as AWS Direct Connect Access to leading peering exchanges such as CoreSite's Any2Exchange® for Internet peering, New York International Internet eXchange (NYIIX), and Deutscher Commercial Internet Exchange (DE-CIX) New York
Deployments	Cabinets and cages Rooftop space available
Fit Out	Turn-key
Power	AC and DC
UPS / PDU / RPP **Generators**	N and 2N redundancy N+1 redundancy
Security	Key card access Biometric scanners Double mantrap entry Perimeter and interior IP-DVR cameras 24x7x365 security guard monitoring Controlled site access

NY2	
CoreSite's NY2 facility is a scalable and reliable data center solution for enterprises looking to expand and reduce costs in the New York metro area, while optimizing performance with direct, low-latency campus access to CoreSite's NY1 facility in the digital center of Manhattan.	
Features / Size	236,000+ square feet of data center space built above the 500-year flood plain Access to the CoreSite Open Cloud Exchange, as well as leading cloud providers such as AWS Direct Connect Access to Any2 Exchange® for Internet peering, NYIIX, and DE-CIX New York
Deployments	Cabinets, cages, private suites, and build-to-suit Rooftop space available
Fit Out	Powered shell, infrastructure shell, and turn-key
Power	AC and DC
UPS / PDU / RPP **Generators**	N, N+1, and 2N redundancy N+1 redundancy
Certifications	Energy Star
Security	Key card access Biometric scanners Double mantrap entries Perimeter and interior IP-DVR cameras 24x7x365 security by CoreSite security officers 8' perimeter fence with controlled site access
Reston Campus (VA1 and VA2)	
CoreSite's Reston data center campus includes two facilities, VA1 and VA2. The campus is designed to create a scalable and reliable option for enterprises, networks, and cloud providers looking to expand operations and reduce costs with direct, low-latency access to and from Ashburn and Washington, D.C.	
Features / Size	390,000+ square feet of data center space Access to over 125 network, cloud, and IT service providers Metro connectivity to DC1 in Washington, D.C. Access to the CoreSite Open Cloud Exchange and Any2Exchange® for Internet peering, as well as leading cloud providers such as AWS Direct Connect
Deployments	Cabinets, cages, private suites, and build-to-suit Rooftop space available
Fit Out	Turn-key
Power	AC and DC
UPS / PDU / RPP **Generators**	N, N+1, 2N redundancy N+1 redundancy
Security	Key card access Biometric scanners Double mantrap entries Perimeter and interior IP-DVR cameras 24x7x365 security by CoreSite security officers Controlled site access

DC1	
CoreSite's DC1 data center is in the K Street corridor, offering unmatched proximity to government agencies and financial institutions. DC1's Tier 1 carrier connectivity enables customers to deploy mission critical applications and network points of presence in Washington, D.C., and to scale via direct access to CoreSite's Reston, Virginia (VA) campus.	
Features / Size	22,000+ square feet of data center space Access to over 125 network, cloud, and IT service providers Diverse dark fiber and dense wavelength division multiplexing (DWDM) connectivity to CoreSite's Reston, VA campus Access to the CoreSite Open Cloud Exchange and Any2Exchange® for Internet peering, as well as leading cloud providers such as AWS Direct Connect
Deployments	Cabinets and cages Rooftop space available
Fit Out	Turn-key
Power	AC and DC
UPS / PDU / RPP **Generators**	N, 2N redundancy N+1 redundancy
Security	Key card access Biometric scanners Camera-monitored entries Perimeter and interior IP-DVR cameras 24x7x365 remote security monitoring Controlled site access
CH1	
CoreSite's CH1 facility is strategically located in downtown Chicago, adjacent to the Board of Trade. This centralized location offers the many financial, healthcare, and media companies deployed within CH1 low-latency connections to local exchanges and communication hubs.	
Features / Size	178,000+ square feet of data center space Access to over 55 network, cloud, and IT service providers Access to the CoreSite Open Cloud Exchange and Any2Exchange® for Internet peering
Deployments	Cabinets, cages, and private suites Rooftop space available
Fit Out	Turn-key
Power	AC and DC
UPS / PDU / RPP **Generators**	N, N+1, 2N redundancy N+1 redundancy
Security	Key card access Biometric scanners Mantrap entries Perimeter and interior IP-DVR cameras 24x7x365 security guard monitoring Controlled site access

SV1	
CoreSite's SV1 facility serves as the carrier hub for CoreSite's tethered Silicon Valley data center campus. The Silicon Valley campus (SV1, SV2, SV3, SV4, and SV7) includes over 185 customers, including international and national carriers, social media companies, cloud computing providers, media and entertainment firms and enterprises.	
Features / Size	85,000+ square feet of data center space Critical data center gateway for subsea cables to the Asia Pacific market Access to the CoreSite Open Cloud Exchange as well as leading cloud services such as AWS Direct Connect Access to Any2Exchange® for Internet peering and Amsterdam Internet Exchange (AMS-IX) Bay Area
Deployments	Cabinets, cages, and private suites Rooftop space available
Fit Out	Turn-key
Power	AC and DC
UPS / PDU / RPP **Generators**	N, N+1, 2N redundancy N redundancy
Security	Key card access Biometric scanners Perimeter and interior IP-DVR cameras 24x7x365 security guard monitoring Controlled site access
SV2	
CoreSite's SV2 facility, part of CoreSite's Silicon Valley campus, brings together native carriers, strong cloud service solutions, and high-density colocation services to serve a data center customer community comprised of gaming and digital content creators, social media networks, enterprises, and CDNs.	
Features / Size	76,600+ square feet of data center space Centrally located in the heart of the world's most influential technology companies Access to the CoreSite Open Cloud Exchange as well as leading cloud services such as AWS Direct Connect Access to Any2Exchange® for Internet peering and AMS-IX Bay Area
Deployments	Cabinets, cages, and private suites Rooftop space available
Fit Out	Turn-key
Power	AC and DC
UPS / PDU / RPP **Generators**	N, N+1, 2N redundancy N+1 redundancy
Security	Key card access Biometric scanners Mantrap entries Perimeter and interior IP-DVR cameras 24x7x365 security guard monitoring 8' perimeter fence with controlled site access

SV3	
CoreSite's Silicon Valley data center campus is centrally located between economic centers such as Palo Alto, San Jose, Redwood City, and Cupertino. The CoreSite SV3 data center in Santa Clara features over 50,000 square feet of space as well as access to the CoreSite Open Cloud Exchange and Any2Exchange® for Internet peering.	
Features / Size	50,000+ square feet of data center space
Deployments	Cages and private suites
Fit Out	Turn-key
Power	AC and DC
UPS / PDU / RPP **Generators**	N, N+1, 2N redundancy N+1 redundancy
Security	Key card access Security guard station at the facility main entrance Biometric scanners Perimeter and interior IP-DVR cameras 8' perimeter fence with controlled site access
SV4	
CoreSite's SV4 facility, part of the Santa Clara campus in the Silicon Valley market, is comprised of 101,000 square feet of space with the ability to expand on campus to meet the business application needs of customers. SV4 includes access to regional, national, and global providers on-site, as well as direct access to the network, cloud, and enterprise community across the rest of CoreSite's Silicon Valley market.	
Features / Size	101,000+ square feet of data center space Access to the CoreSite Open Cloud Exchange as well as leading cloud services such as AWS Direct Connect Access to Any2Exchange® for Internet peering and AMS-IX Bay Area
Deployments	Cabinets, cages, private suites, and build-to-suit Rooftop space available
Fit Out	Turn-key
Power	AC and DC
UPS / PDU / RPP **Generators**	N, 2N redundancy N+1 redundancy
Security	Key card access Biometric scanners Mantrap entries Perimeter and interior IP-DVR cameras 24x7x365 security guard monitoring 8' perimeter fence with controlled site access

SV7	
CoreSite's SV7 facility features the latest in data center efficiency and redundancy designs. The facility offers access to the network, cloud, and enterprise community across CoreSite's Santa Clara campus and the rest of CoreSite's Silicon Valley data center market.	
Features / Size	615,000+ sq. ft. of data center space Access to Any2Exchange® for Internet peering and AMS-IX Bay Area Access to the CoreSite Open Cloud Exchange as well as native access to AWS Direct Connect
Developments	Cabinets, cages, private suites, and build-to-suit Rooftop space available
Fit Out	Powered shell, infrastructure shell, and turn-key
Power	AC and DC
UPS / PDU / RPP **Generators**	N, 2N redundancy N+1 redundancy
Security	Key cards and biometric scanners Mantrap entries 8' Perimeter fence and controlled site access Perimeter and interior IP-DVR 24x7x365 in-house staffed
LA1	
CoreSite's LA1 facility, also known as One Wilshire®, is one of the most densely interconnected data centers in the world. Home to over 350 network, cloud, and IT service providers, the LA1 provides access to a multitude of interconnections and service partners for its customer ecosystem.	
Features / Size	149,000+ square feet of data center space Tethered to CoreSite's LA2 data center via high-count dark-fiber Native access to the CoreSite Open Cloud Exchange and Any2Exchange® for Internet peering, as well as leading cloud services such as AWS Direct Connect and Microsoft Azure ExpressRoute Industry-leading connectivity to Asia-Pacific markets
Deployments	Cabinets, cages, and private suites Rooftop space available
Fit Out	Turn-key
Power	AC and DC
UPS / PDU / RPP **Generators**	N, N+1, 2N redundancy N+1 redundancy
Security	Key card access Biometric scanners Double mantrap entry Perimeter and interior IP-DVR cameras 24x7x365 remote security monitoring Controlled site access

LA2	
CoreSite's LA2 facility provides data center scalability within the Los Angeles market. Over 350 national and international networks and cloud providers serve the ecosystem of entertainment companies, digital content providers, and CDNs that make up CoreSite's LA market.	
Features / Size	424,000+ square feet of data center space Tethered to CoreSite's LA campus via high-count dark-fiber Access to the CoreSite Open Cloud Exchange and Any2Exchange® for Internet peering, as well as leading cloud services such as AWS Direct Connect and Microsoft Azure ExpressRoute
Deployments	Cabinets, cages, private suites, and build-to-suit Rooftop space available
Fit Out	Powered shell, infrastructure shell, and turn-key
Power	AC and DC
UPS / PDU / RPP **Generators**	N, N+1, 2N redundancy N+1 redundancy
Security	Key card access Biometric scanners Double mantrap entry Perimeter and interior IP-DVR cameras 24x7x365 security guard monitoring 8' perimeter fence with controlled site access
DE1	
CoreSite's DE1 data center is in downtown Denver's landmark Gas and Electric Building, which sits at the nexus of multiple fiber plants for national and regional network service providers. DE1 offers access to the CoreSite Any2Exchange® for Internet peering (formerly the Rocky Mountain Internet Exchange), the largest peering exchange in the region.	
Features / Size	14,000+ square feet of data center space Access to over 75 network, cloud, and IT service providers Tethered to CoreSite's DE2 data center via dark fiber
Deployments	Cages, full, half, third, and quarter cabinets
Fit Out	Turn-key
Power	AC and DC
UPS / PDU / RPP **Generators**	N, 2N redundancy N+1 redundancy
Security	Key card access Biometric scanners Interior IP-DVR cameras Controlled site access

DE2	
CoreSite's DE2 data center is located adjacent to Level 3 Communications gateway facility and provides seamless access to the major carriers serving the Rocky Mountain region.	
Features / Size	5,100+ square feet of data center space Tethered to CoreSite's DE1 data center via dark fiber Access to over 75 network, cloud, and IT service providers Access to the CoreSite Any2Exchange® for Internet peering (formerly the Rocky Mountain Internet Exchange), the largest peering exchange in the region
Deployments	Full, half, and quarter cabinets Rooftop space available
Fit Out	Turn-key
Power	AC and DC
UPS / PDU / RPP **Generators**	N, 2N redundancy N redundancy
Security	Key card access Biometric scanners Interior IP-DVR cameras Controlled site access

CoreSite provides customers with cross connections and Any2 Peering Exchange opportunities including the following:

Cross Connections

A cross-connect is an A-Z connection that is either "dark or passive" as in a pair of single-mode optical fiber (SMF), coax, or CAT-5/6 cable or an "optical or electrical", switched-multiplexed service with a provisioned bit rate within a CoreSite intra or inter-facility transmission equipment. A-Z is defined as customer-to-customer or customer-to-carrier. Electrical signals such as digital signal 1 (DS-1) from customers to other customers or carriers are limited to about 350 linear feet of transmission medium. For distances greater than 350 feet, CoreSite converts the electronic signal over fiber optics connecting higher order Telco grade multiplexers or media converters. CoreSite provides intra-site Ethernet connectivity via a combination of core and edge switches.

CoreSite interconnects its enterprise and carrier hotel colocation data centers within a metro market area in order to provide Ethernet and synchronous optical networking (SONET) / time-division multiplexing (TDM) interconnection services between data centers. CoreSite's network policy when interconnecting data centers is to use diverse dark fiber (DF) pairs connected to separate DWDM line cards on a single DWDM chassis.

Any2 Peering Exchange

Any2 is a layer 2, Internet Protocol version 6 (IPv6)-supporting, physical network switch operated by CoreSite to facilitate the exchange of Internet traffic between Internet service providers (ISPs) and content creators and providers. It is a place for network providers to interconnect and exchange IP traffic at a local or international level by means of mutual peering agreements. To facilitate access to the 'global Internet,' a network, or ISP must have connectivity to the global Internet itself and a registered autonomous system (AS) number from a regional Internet registry such as American Registry for Internet Numbers (ARIN) or Réseaux IP Européens (RIPE).

In addition to classic exchange point utilities, Any2 Exchange also fully supports IPv6 throughout the exchange infrastructure, reverse domain name service (DNS) lookup, and no cost IPv6 address support to customers. Any2Easy route servers in California are supporting more than 100 networks, and have an average of 20,000 routes available at any time. Any2 welcomes remote access networks (those networks without a physical point of presence (POP) within a CoreSite data center) and is open to further federation with other non-profit or regional exchanges.

System Boundaries

As outlined in the 2016 TSP section 100A, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy,* a system is designed, implemented, and operated to achieve specific business objectives (for example, delivery of services, production of goods) in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures and data.

The scope of this report includes reliability of data center power, reliability of data center cooling, security of premises, and technical support to customers for the following 17 CoreSite data center facilities:

Metro Area	Name	Address
Boston	BO1	70 Inner Belt Road, Somerville, Massachusetts 02143
Chicago	CH1	417 South LaSalle Street, Chicago, Illinois 60602
Washington, D.C.	DC1	1275 K Street NW, Suite 700, Washington D.C. 20005
Denver	DE1	910 15th Street, Denver, Colorado 80202
Denver	DE2	639 East 18th Avenue, Denver, Colorado 80203
Los Angeles	LA1	624 South Grand Avenue (One Wilshire Boulevard), Los Angeles, California 90017
Los Angeles	LA2	900 North Alameda Street, Los Angeles, California 90012
Miami	MI1	2115 NW 22nd Street, Miami, Florida 33142
New York City	NY1	32 Avenue of the Americas, New York, New York 10013
Secaucus	NY2	2 Emerson Lane, Secaucus, New Jersey 07094
Reston	VA1	12100 Sunrise Valley Drive, Reston, Virginia 20191
Reston	VA2	12098 Sunrise Valley Drive, Reston, Virginia 20191
San Jose	SV1	55 South Market Street, San Jose, California 95113
Milpitas	SV2	1656 McCarthy Boulevard, Milpitas, California 95035
Santa Clara	SV3	2901 Coronado Drive, Santa Clara, California 95054
Santa Clara	SV4	2972 Stender Way, Santa Clara, California 95054
Santa Clara	SV7	3020 Coronado Drive, Santa Clara, California 95054

Infrastructure and Software

The physical and environmental security infrastructure that supports the CoreSite colocation services includes primary and secondary systems. For the physical security safeguards provided by the system, CoreSite utilizes the Lenel OnGuard (Lenel) badge access control system to detect unauthorized access attempts to and within the colocation facilities. The badge access control system enforces two-factor authentication via badge access combined with biometric readers in order to access the customer infrastructure (e.g. raised floor / production areas) within the colocation facilities. The production servers and databases supporting the badge access control system are Windows-based with their access and authentication controls integrated with and inherited from Microsoft Active Directory. Authorized users can remotely access the production network via transport layer security (TLS) encrypted virtual private network (VPN) connections. Once authenticated to the VPN or corporate network, users are required to utilize jump servers requiring multi-factor authentication (MFA) in order to access the production environment (e.g. servers and databases). Multiple Check Point firewall systems are in place over the production network, which are configured as failover clusters for high availability in the event of a primary firewall failure. The badge access control system and supporting network infrastructure are considered primary systems.

Additionally, CoreSite utilizes network video recorder (NVR) camera systems to continuously record and monitor unauthorized access/activity within the colocation facilities. The NVR camera systems are networked to an enterprise-wide system to provide for off-site monitoring capabilities.

The badge access control system and NVR camera systems are maintained and monitored at each individual colocation facility and are also capable of being monitored remotely. These systems are utilized to capture, and, in conjunction with review by CoreSite's functional groups, address significant events and conditions related to the colocation services provided by CoreSite. The historical logs from these systems are maintained for at least 90 days for audit and review purposes.

For environmental security safeguards, CoreSite utilizes building automation systems to detect and report on environmental conditions within the colocation facilities. Specifically, the building automation systems are utilized for the monitoring of electronic power and cooling systems within the colocation facilities, including, but not limited to, the following: generators, UPS systems, redundant substation connectivity, chillers, pumps, computer room air handler (CRAH) units, and computer room air conditioning (CRAC) units. The building automation systems are configured to alert data center facilities and operations personnel when predefined thresholds are exceeded or alarms are triggered on monitored devices.

Additionally, CoreSite utilizes an automated ticketing system to process and track internal and external requests related to change requests, incidents, work orders, trouble tickets, remote hands, service appointments, deliveries, property removal, construction, and access requests, modifications, and deletions.

The NVR camera systems, building automation systems, and automated ticketing systems are considered secondary systems used to support and facilitate providing the colocation services. The controls related to the maintenance and logical access to these systems are likely not relevant to the common information needs of a broad range of users of the colocation services. As a result, CoreSite has determined the controls specific to the NVR camera systems, building automation systems, and automated ticketing system to be outside the boundaries of the system.

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**
Lenel Badge Access Control System	Third party developed badge access control system utilized to control access to and monitor the security of the data center facilities. Sensitive areas containing customer infrastructure require two-factor authentication protocols consisting of badge access and biometric readers	Windows VMware Virtual Platform	Reston, Virginia; Los Angeles, California
Active Directory	Utilized to manage user accounts and authentication requirements for the production network, including the servers and databases supporting the Lenel access control system	Windows Virtual Machine	Denver, Colorado
Production Servers and Databases	Application and database servers supporting the Lenel access control system	Windows VMware Virtual Platform; Microsoft SQL Server	Reston, Virginia; Los Angeles, California
Jump Servers	Jump servers requiring MFA utilized to access the production servers and databases	Windows VMware Server 2012 R2	Los Angeles, California; Denver, Colorado

Primary Infrastructure			
Production Application	**Business Function Description**	**Operating System Platform**	**Physical Location**
Firewall System	Utilized to filter and route traffic to and from the production network	Check Point	Reston, Virginia; Los Angeles, California; Denver, Colorado
VPN	Encrypted VPNs utilized for remote access to the production network	Windows Virtual Machine	Denver, Colorado

People

CoreSite utilizes the following functional areas of operations within the scope of this review:

- Executive management – responsible for overseeing company-wide activities, establishing and accomplishing goals, and overseeing objectives
- Field operations – responsible for overseeing day-to-day operations of the data center facilities and responding to customer inquiries
- Security group – responsible for monitoring the physical security of the data center facilities 24 hours per day

Procedures

Physical Security

CoreSite maintains a standard operating procedures (SOP) manual to address security procedures for its colocation facilities. The security SOP identifies roles and responsibilities of colocation staff and members of the security team and addresses topics such as visitor management, deliveries, property and equipment removal, management of the access control system, handling of customer's proprietary infrastructure, and incident response. The security SOP also contains site risk assessment forms to allow for the identification and mitigation of location-specific risks.

Colocation facilities are supported by both manual and automated controls to help ensure the premises remain secure. On-site internal or third party (CH1 only) security guards monitor physical security at all of the in-scope colocation facilities excluding DE2. For DE2, the physical security of the colocation facilities is monitored remotely 24 hours per day by the LA2 CoreSite security team. Additionally, badge access control systems are in place to control access to and within the colocation facilities. To access the customer infrastructure (e.g. raised floor or production areas) at each colocation facility, the badge access control system enforces two-factor authentication by requiring a biometric scan in addition to a badge. The badge access control systems are configured to log ingress and egress activity at colocation facilities, maintaining a history for at least 90 days for review purposes. Additionally, the badge access control system is configured to alert security personnel upon certain physical security events that have occurred, such as door held open or biometric mismatch alerts.

Employee badge access privileges are granted based on individual job responsibilities and revoked as a component of the termination processes. Physical access reviews are performed for each colocation facility on a semi-annual basis to help ensure that access to the data centers is restricted to authorized personnel. Physical access requests for external users (e.g. customers, contractors, vendors, etc.) are documented on an access request ticket within the automated ticketing system and are required to be submitted to facilities security personnel for processing. The ability to administer the badge access control systems is restricted to user accounts accessible by authorized personnel. Visitors to colocation facilities are required to provide photo identification, to be logged in the badge access systems, sign a visitor log, and are issued a temporary badge for use while within the colocation facilities. Historical visitor logs are retained for a minimum of 90 days for review

purposes. Physical key inventory listings are maintained, as applicable, to track physical key assignments. Additionally, visitors require an escort at all times.

Data center staff utilize an automated ticketing system to process and track requests related to service appointments, deliveries, property removal, construction, and access requests modifications and deletions. Deliveries to colocation facilities are required to be logged into the ticketing system. Security of the colocation facilities is further enabled via the use of NVR camera systems which are in place to monitor activity to and throughout the colocation facilities. NVR images are retained for a minimum of 90 days for review purposes. Lastly, alarm panels are in place within the colocation facilities and security guards are alerted when an alarm panel is triggered.

Logical Security

The in-scope systems (e.g. Lenel production servers and databases, jump servers, VPN, firewall systems, Lenel application) are configured to authenticate users with a user account and enforce predefined user account and minimum password requirements. Each system is integrated with and inherit their authentication settings from the network domain (Active Directory). Once logged into the VPN or corporate network, users must authenticate into jump servers using MFA, in order to access the production environment, where the Lenel production servers and databases reside.

The in-scope systems utilize predefined security groups to assign role-based access privileges and segregate access to data. Administrative access privileges to the in-scope systems are restricted to user accounts accessible by authorized personnel. On a semi-annual basis, user access reviews, which include privileged user accounts of the network domain, are performed to help ensure that access to data is restricted and provides for appropriate segregation of duties. A termination ticket is completed and systems access is revoked for employees as a component of the employee termination process.

Network Monitoring and Security

CoreSite's IT security group monitors the security impact of emerging technologies via security subscriptions and bulletins and the impact of applicable laws or regulations are considered by senior management. On a weekly basis, CoreSite IT personnel utilize the Nexpose Rapid7 product to perform automated internal vulnerability scans of the production servers. Remediation plans are documented within the automated ticketing system and monitored through resolution, where necessary.

A Check Point firewall system is in place to filter unauthorized inbound network traffic from the Internet. The firewall system is comprised of three clusters for high availability to provide failover firewall services in the event of a primary firewall failure. On a quarterly basis, firewall rules are reviewed to help ensure that only necessary connections are configured within the rulesets. Firewall ruleset changes are required to be documented within the automated ticketing system and approved prior to implementation. Trend Micro antivirus software is utilized to protect registered production Windows servers and workstations. The antivirus software is configured to scan for updates to virus definitions and upgrade registered clients on a daily basis as well as scan registered clients on a weekly basis.

Data Transmission

A data classification procedure is in place that prohibits the transmission of sensitive and/or confidential information over the Internet or other public communications paths unless it is encrypted. For remote access to the production network, TLS encrypted VPNs are required which are integrated with and inherit their predefined user account and minimum password requirements from the network domain. VPN access is revoked upon employee termination.

Incident Response

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. Additionally, policies are documented and maintained that address remedial actions for lack of compliance with policies and procedures. Management meetings are held on a quarterly basis to discuss incidents and corrective measures to help ensure that incidents are resolved.

Help desk and operations personnel utilize the automated ticketing system to document information security violations, responses, and resolution. Incidents requiring a change to the system follow the standard change control process.

Change Management

Documented change management policies and procedures are in place to guide personnel in the request, documentation, testing, and approval of system changes. Documented standard build procedures are utilized for installation and maintenance of production servers and infrastructure supporting the badge access control system and include use of an access control system to restrict access to authorized users.

The Lenel badge access control system is a third party developed application and as such, the vendor is responsible for performing application design and development activities. CoreSite performs application updates and operating system server patches and upgrades when new vendor application versions are available. CoreSite utilizes an automated ticketing system to document the authorization, testing, and approvals prior to implementation. Additionally, CoreSite personnel perform a post-implementation review of application updates to help ensure the proper functioning of the application in the production environment.

The ability to promote application updates and operating system patches and upgrades into the production environment is restricted to user accounts accessible by authorized personnel.

Automated backup systems are in place to perform scheduled backups of production servers at predefined times to allow for rollback of changes when updates impair system operation.

Backup Power Infrastructure

CoreSite has controls in place to support the reliability of data center power provided to its colocation facilities. Power availability is contracted with clients during the client setup process based on the client's individual requirements. Colocation facilities maintain a power infrastructure that provides redundancy in power systems. This is accomplished using UPS systems and backup generators at the colocation facilities. UPS systems are configured to ensure power supplies remain uninterrupted with a combination of N, N+1, and 2N configurations at the various colocation facilities. These redundant UPS systems are in place to provide temporary power in the event of a power failure and to mitigate the risk of power surges impacting infrastructure in the colocation facilities. To facilitate the continuous operation of the UPS systems, management ensures that third party vendors inspect the UPS systems on at least an annual basis to help ensure proper functioning.

In addition to UPS systems, the colocation facilities are equipped with single or multiple generators configured to provide temporary power in the event of a failure of the primary power source. Internal personnel inspect the generators owned and managed by CoreSite monthly to ensure proper functioning. Team members utilize a standard checklist to test generator functions, and management supplements these internal reviews with quarterly reviews by third party vendors. Building management is responsible for the maintenance and monitoring of the generator at the DE1 data center facility.

Building automation systems are utilized by data center operations staff to monitor the power supply infrastructure. The building automation systems are configured to alert operations staff when predefined alarms are triggered by a change in conditions of the UPS systems, switches, generators, and other infrastructure that supports power supplied to the colocation facilities.

Cooling, Fire Detection, and Fire Suppression Infrastructure

CoreSite has controls in place to support the reliability of data center cooling for its colocation facilities. CoreSite utilizes multiple air conditioners and/or handlers to cool the colocation facilities and prevent a single point failure. To facilitate consistent operation of cooling equipment, management ensures third party vendors or internal personnel inspect cooling equipment on a quarterly basis. Additionally, the building automation systems are configured to monitor environmental conditions, such as temperature and humidity levels, to help ensure that environmental conditions within the colocation facilities do not exceed predefined thresholds for temperature and humidity. The building automation systems are configured to alert field operations personnel when predefined thresholds are exceeded on monitored devices so that appropriate action can be taken to return data center cooling equipment to normal status.

In addition to data center cooling equipment, colocation facilities are equipped with fire detection and suppression devices that include audible and visual fire alarms, dry-pipe water sprinklers or FM-200 fire suppression systems, fire and smoke detectors, and hand-held fire extinguishers. To facilitate the consistent operation of these devices, management ensures that third party vendors inspect the fire detection and suppression equipment on at least an annual basis.

Management Monitoring

Members of the capacity planning team utilize automated monitoring tools and reports to monitor the power and utilization levels of the colocation facilities and supporting infrastructure on a real-time basis. In addition to real-time capacity monitoring, management meetings are held on a quarterly basis to review availability trends and availability forecasts as compared to system commitments.

Production Server Monitoring, Backups, and Database Log Shipping

CoreSite IT personnel utilize the SolarWinds enterprise monitoring application, which is configured to monitor the in-scope production servers' capacity levels and alert IT personnel when predefined thresholds have been met.

Veeam Backup & Replication software is utilized to perform daily, incremental and weekly, full backups of the production servers and alert IT personnel via e-mail regarding backup job completion status.

Transaction log backup files are log shipped every 15 minutes from the primary production database in Reston, Virginia, to a secondary, standby server located in Los Angeles, California, over a private connection, which is not accessible from the public Internet. IT personnel are notified upon failures of the log shipping process via e-mail for proactive monitoring of the log shipping process. Maintaining a warm copy of the production database at an alternate location helps ensure that the production database files will be available despite the loss of or disruptions to, the master database.

Database Restorations and Disaster Recovery

IT personnel perform restoration tests of production server backup files from the most recent differential and full backups on at least an annual basis to help ensure that the production server data is recoverable from the backup files in the event of an outage or declared disaster.

Additionally, business continuity and disaster recovery plans are in place for the corporate headquarters and each individual colocation facility to guide personnel in procedures to protect against disruptions caused by an unexpected event. The plans are tested on at least an annual basis.

Data

CoreSite does not manage customer data being stored within CoreSite's colocation services system. All physical and environmental data is managed and monitored at the individual CoreSite data center facilities as well as by the CoreSite headquarters in Denver, Colorado, by field operations personnel. A centralized badge access control system provides controlled access to the colocation facilities. NVR camera systems are utilized to monitor for intrusion activities or possible vulnerabilities. The badge access control system and NVR camera systems are configured to retain the logs and digital recordings, respectively, for investigations.

The environment, including temperature and humidity in the colocation facilities, is controlled using cooling equipment that is regularly maintained and inspected by third party and internal personnel. Multiple generators and UPS systems are in place at the colocation facilities which are configured to provide redundancy for power systems. The temperature and humidity levels, electrical system, utility power, and distribution systems are monitored using the building automation systems. The building automation systems generate alarms and alert notifications for possible failure or overloading of the power systems.

Significant Changes During the Review Period

The SV7 data center was placed into service on October 12, 2016. The testing of operating effectiveness of the control activities within the security and availability principles specific to SV7 were excluded from the scope of this

report for the period of July 1, 2016, through October 12, 2016 (the period prior to the service go-live date for SV7).

Subservice Organizations

No subservice organizations were included in the scope of this assessment. Therefore, the description does not address the criteria in Section 2, items (a)(i)(4), (a)(i)(5)(b) and (a)(i)(6).

CONTROL ENVIRONMENT

The control environment at CoreSite 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, Audit Committee, 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 CoreSite's control environment affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of CoreSite's ethical and behavioral standards, how they are communicated, and how they are reinforced in practice. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well by example.

Specific control activities that the service organization has implemented in this area are described below.

- Documented organizational policy statements and employee procedures communicate entity values and behavioral standards to personnel.
- Background checks are performed for employees as a component of the hiring process.
- Employees sign an acknowledgment form upon hire indicating that they have been given access to the employee handbook and understand their responsibility for adhering to the code of business conduct and ethics.
- Employees are required to complete ethics training on an annual basis to understand their obligations and responsibilities to comply with the corporate code of business conduct and ethics.

Board of Directors and Audit Committee Oversight

CoreSite's control consciousness is influenced significantly by its Board of Directors and Audit Committee. The Board of Directors and Audit Committee are in place to oversee management activities and meet on a regular basis to discuss matters pertinent to the organization's operations and to review financial results. External audits are performed by various independent third parties to monitor the company's compliance with regulatory requirements.

Organizational Structure and Assignment of Authority and Responsibility

CoreSite's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. CoreSite's management believes that establishing a relevant organizational structure includes considering key areas of authority and responsibility and lines of reporting. CoreSite 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.

CoreSite'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 the defined key areas of authority, responsibility and lines of reporting to personnel related to the design, development, implementation, operation, maintenance, and monitoring of the system. These charts are communicated to employees via a secure file sharing application intranet and updated as needed.

Commitment to Competence

CoreSite's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Human resources (HR) personnel consider the competence levels for particular jobs and translate the required skills and knowledge levels into written position requirements. Training courses are available to new and existing employees to maintain and advance the skill level of personnel. An automated compliance monitoring system is in place to track employee compliance with training requirements.

Accountability

CoreSite's management philosophy and operating style encompass 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. Bi-weekly meetings are scheduled to discuss issues with the field operations management team.

CoreSite's HR policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that the service organization has implemented in this area are described below.

- New employee hiring procedures, including the use of new hire checklists, are in place to guide the hiring process and include verification that candidates possess the required qualifications to perform the duties as outlined in the job description.
- Evaluations are performed for each employee on an annual basis.
- 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.
- Documented policies and procedures are in place that address remedial actions for lack of compliance with policies and procedures.
- A termination checklist is completed as a component of the employee termination process.

RISK ASSESSMENT

Risk Identification

Management is responsible for identifying the risks that threaten achievement of the security and availability trust services principles and underlying criteria stated in the management's description of the service organization's system. Management has implemented a process for identifying relevant risks. This process includes estimating the impact of identified risks, assessing the likelihood of their occurrence, and determining actions to address them, including designing, implementing, and documenting control activities to mitigate risks.
CoreSite's management has placed into operation a risk assessment process to identify and manage risks that could affect the organization's ability to achieve organizational objectives including the operation of colocation services for user entities. The process requires management to identify significant risks and to implement appropriate measures to mitigate those risks.

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
- Fraud incentives and pressures for employees
- Fraud opportunities
- Employee attitudes and rationalizations for fraud
- A disruption in information systems processing
- The quality of personnel hired and methods of training utilized
- Changes in management responsibilities

Risk Analysis

Risk analysis includes identification of key business processes where potential exposures of some consequence exist. Once the significance and likelihood of a 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. On at least an annual basis, CoreSite's processes are analyzed against the risk factors and assigned a risk ranking of low, medium, or high. The risk analysis is reviewed by members of management and an action plan is developed to mitigate identified risks.

TRUST SERVICES CRITERIA AND RELATED CONTROL ACTIVITIES

Integration with Risk Assessment

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

Selection and Development of Control Activities

The applicable trust criteria and related control activities are included in Section 4 of this report to eliminate the redundancy that would result from listing the items in this section and repeating them in Section 4. Although the applicable trust criteria and related control activities are included in Section 4, they are, nevertheless, an integral part of CoreSite'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 principles are applicable to the colocation services system. Therefore, the description does not address the (a)(i)(7) criteria in Section 2.

INFORMATION AND COMMUNICATION SYSTEMS

Relevant Information

Information is necessary for CoreSite to carry out internal control responsibilities to support the achievement of its objectives related to the colocation services system. Management obtains or generates and uses relevant and quality information from both internal and external sources to support the functioning of internal control.

The following provides a summary of internal and external sources of information used in the colocation services:

- The Lenel badge access system is used to identify individuals authorized to access the data center facilities and provide activity logs to help monitor successful and unsuccessful access attempts. Additionally, these systems provide alerts regarding potential security violations for review by on-site and central security personnel.
- The NVR camera systems are used to monitor and record activity at the data center facilities.
- The building automation systems provide alerts and reporting regarding the environmental security equipment at the data center facilities.
- E-mail and the automated ticketing systems are used to communicate with internal and external / customer personnel regarding services provided, work orders requested / processed, etc.

Communication

Upper management is involved with day-to-day operations and can provide personnel with an understanding of their individual roles and responsibilities pertaining to internal controls. This includes the extent to which personnel understand how their activities relate to the work of others and the means of reporting exceptions to higher level personnel within the company. CoreSite management believes that open communication channels help ensure that exceptions are reported and acted on. For that reason, formal communication tools such as employee handbooks are in place. Management's communication activities are made electronically, verbally, and through the actions of management.

MONITORING

Monitoring is a process that assesses the quality of internal control performance over time. It involves assessing the design and operation of controls and taking necessary corrective actions. This process is accomplished through ongoing activities, separate evaluation, or a combination of the two. Monitoring activities also include using information from communications from external parties such as user entity complaints and regulatory comments that may indicate problems or highlight areas in need of improvement. Management has implemented a self-assessment and compliance program to ensure the controls are consistently applied as designed.

Ongoing Monitoring

Automated and manual systems are utilized to identify deviations from standards for physical and environmental security control systems. Additionally, CoreSite personnel use automated systems to monitor customer devices in accordance with contractual requirements and service level agreements. Management's close involvement in operations helps to identify significant variances from expectations regarding internal controls. Upper management immediately evaluates the specific facts and circumstances related to any suspected control breakdowns. A decision for addressing any control weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel.

Separate Evaluations

Management has implemented a self-assessment program to evaluate the performance of specific control activities and processes over time, and confirm that the in-scope controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority. As a result of management's risk analysis process, each control activity within scope has been assigned a risk level associated with the assessed level of risk it is intended to mitigate. Controls that serve to mitigate multiple risks are assigned the highest level of assessed risk among the pertinent risks.

Internal and External Auditing

CoreSite supports many user entities in their efforts to meet the regulatory demands of their industry or governing agency. CoreSite has assisted user entities in successfully meeting the requirements of many certifications and regulatory demands, including:

- Type 2 System and Organization Controls (SOC 1) examinations
- Type 2 SOC 2 examinations
- International Organization of Standardization (ISO) / International Electrotechnical Commission (IEC) 27001 certification and surveillance reviews
- Payment Card Industry (PCI) Data Security Standard (DSS) validations
- Sarbanes-Oxley (SOX)

Internal Audit conducts data center reviews based on a data center specific risk assessment performed on at least an annual basis. Testing is performed to ensure documented operating procedures are operating effectively and areas of high risk are addressed. Data center audit reports are issued and escalated as appropriate.

The Internal Audit staff reports to the Audit Committee which is comprised of a subset of the members of the Board of Directors. The Audit Committee ensures the Internal Audit Department is appropriately staffed and qualified. The Audit Committee also provides direction and oversight of the department's engagements, reviews results, and monitors resolution of noted issues.

An external audit firm is engaged to review financial results and other Securities Exchange Commission (SEC) required filings. This firm is reviewed and approved annually by the shareholders and meets regularly with the Audit Committee and larger Board of Directors. Review of the external audit firm includes ensuring appropriate experience and compensation levels. Both internal and external auditors are required to maintain levels of independence.

Evaluating and Communicating Deficiencies

Management has developed protocols to ensure findings of internal control deficiencies should be reported to operational and corporate management. This process enables individuals to provide needed support or oversight for taking corrective action and to communicate with others in the organization whose activities may be affected. Any deficiencies are investigated by CoreSite's management team members and, if necessary, are reported to the senior management team or the Board of Directors. Further, deficiencies are recorded and tracked through resolution by Internal Audit.

COMPLEMENTARY CONTROLS AT USER ENTITIES

Complementary user entity controls are not required, or significant, to achieve the applicable trust services criteria. Therefore, the description does not address the (a)(i)(5)(a) criteria in Section 2.

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 CoreSite. 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 July 1, 2016, to June 30, 2017.

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.

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 PRINCIPLE AND CRITERIA TABLE

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.0: Common Criteria Related to Organization and Management			
CC1.1: The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system enabling it to meet its commitments and system requirements as they relate to security and availability.			
CC1.1.1	Organizational charts are in place to communicate the defined key areas of authority, responsibility and lines of reporting to personnel related to the design, development, implementation, operation, maintenance, and monitoring of the system. These charts are communicated to employees via the company intranet and updated as needed.	Inquired of the compliance manager regarding organizational management to determine that organizational charts were in place, communicated to employees, and updated as needed.	No exceptions noted.
		Inspected the company organizational charts to determine that organizational charts were in place to communicate the defined key areas of authority, responsibility and lines of reporting to personnel related to the design, development, implementation, operation, maintenance, and monitoring of the system and were updated as needed.	No exceptions noted.
		Inspected the organizational charts on the company intranet to determine that organizational charts were communicated to employees via the company intranet.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.1.2	Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.	Inspected the documented position descriptions for a sample of employment positions to determine that documented position descriptions were in place for each employment position sampled to define the skills and knowledge levels required for the competence levels of particular jobs.	No exceptions noted.
CC1.2: Responsibility and accountability for designing, developing, implementing, operating, maintaining, monitoring, and approving the entity's system controls and other risk mitigation strategies are assigned to individuals within the entity with authority to ensure policies and other system requirements are effectively promulgated and implemented to meet the entity's commitments and system requirements as they relate to security and availability.			
CC1.2.1	Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.	Inspected the documented position descriptions for a sample of employment positions to determine that documented position descriptions were in place for each employment position sampled to define the skills and knowledge levels required for the competence levels of particular jobs.	No exceptions noted.
CC1.3: The entity has established procedures to evaluate the competency of personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring the system affecting security and availability and provides resources necessary for personnel to fulfill their responsibilities.			
CC1.3.1	Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.	Inspected the documented position descriptions for a sample of employment positions to determine that documented position descriptions were in place for each employment position sampled to define the skills and knowledge levels required for the competence levels of particular jobs.	No exceptions noted.
CC1.3.2	New employee hiring procedures are in place to guide the hiring process and include verification that candidates possess the required qualifications to perform the duties as outlined in the job description.	Inspected the new employee hiring policies and procedures to determine that new employee hiring procedures were in place to guide the hiring process and included verification that candidates possessed the required qualifications to perform the duties as outlined in the job description.	No exceptions noted.
		Inspected the completed new hire checklists for a sample of employees hired during the review period to determine that verification that candidates possessed the required qualifications to perform the duties as outlined in the job description was documented as performed for each employee sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.3.3	Training courses are available to new and existing employees to maintain and advance the skill level of personnel.	Inquired of the compliance manager regarding employee training to determine that training courses were available to new and existing employees to maintain and advance the skill level of personnel.	No exceptions noted.
		Inspected the automated learning management system training schedule and example course descriptions to determine that training courses were available to new and existing employees to maintain and advance the skill level of personnel.	No exceptions noted.
CC1.3.4	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.	Inquired of the compliance manager regarding security awareness training to determine that employees were 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.	No exceptions noted.
		Inspected the training content and evidence of 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.
CC1.3.5	An automated compliance monitoring system is in place to track employee compliance with training requirements.	Inquired of the compliance manager regarding the monitoring of employee compliance with training requirements to determine that an automated system was in place to track training requirements.	No exceptions noted.
		Inspected the automated learning management system and example compliance reports to determine that an automated learning management system was utilized to track employee compliance with training requirements.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.4: The entity has established workforce conduct standards, implemented workforce candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and system requirements as they relate to security and availability.			
CC1.4.1	Employees sign an acknowledgment form upon hire indicating that they have been given access to the employee handbook and understand their responsibility for adhering to the code of conduct outlined within the handbook.	Inspected the employee handbook and the signed acknowledgments for a sample of employees hired during the review period to determine that each employee sampled signed an acknowledgement indicating that they had been given access to the employee handbook and understood their responsibility for adhering to the code of conduct outlined within the handbook.	No exceptions noted.
CC1.4.2	Employees are required to complete ethics training on an annual basis to understand their obligations and responsibilities to comply with the corporate code of business conduct and ethics.	Inquired of the compliance manager regarding ethics training to determine that employees were required to complete ethics training on an annual basis to understand their obligations and responsibilities to comply with the corporate code of business conduct and ethics.	No exceptions noted.
		Inspected the ethics training content and evidence of training completion for a sample of current employees to determine that each employee sampled completed ethics training during the review period.	No exceptions noted.
CC1.4.3	Background checks are performed for employees as a component of the hiring process.	Inspected the completed background check documentation for a sample of employees hired during the review period to determine that background checks were performed as a component of the hiring process for each employee sampled.	No exceptions noted.
CC2.0: Common Criteria Related to Communications			
CC2.1: Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external users of the system to permit users to understand their role in the system and the results of system operation.			
CC2.1.1	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 authorized users.	Inquired of the compliance manager regarding communication of the system description to determine that a system description was documented that included the services provided, data, people, software, infrastructure, procedures, control environment, risk assessment, monitoring, and information and communication systems, and that it was communicated to authorized users.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the system description and evidence of communication to determine that a system description was documented and included the services provided, data, people, software, infrastructure, procedures, control environment, risk assessment, monitoring, and information and communication systems.	No exceptions noted.
CC2.2: The entity's security and availability commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal users to enable them to carry out their responsibilities.			
CC2.2.1	The entity's security and availability commitments and the associated system requirements are documented and communicated to internal and external users via the following channels: • Customer contracts and nondisclosure agreements • Marketing materials and brochures	Inspected the customer contract and nondisclosure agreement templates as well as example marketing materials and brochures to determine that the entity's security and availability commitments and the associated system requirements were documented and communicated to internal and external users.	No exceptions noted.
CC2.2.2	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.	Inquired of the compliance manager regarding security awareness training to determine that employees were 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.	No exceptions noted.
		Inspected the training content and evidence of 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.
CC2.2.3	Employees are required to complete ethics training on an annual basis to understand their obligations and responsibilities to comply with the corporate code of business conduct and ethics.	Inquired of the compliance manager regarding ethics training to determine that employees were required to complete ethics training on an annual basis to understand their obligations and responsibilities to comply with the corporate code of business conduct and ethics.	No exceptions noted.
		Inspected the ethics training content and evidence of training completion for a sample of current employees to determine that each employee sampled completed ethics training during the review period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.2.4	Documented policies and procedures are in place to guide personnel in the entity's security and availability commitments and the associated system requirements. The policies and procedures are communicated to internal personnel via the company intranet.	Inspected the security policies and employee handbook and evidence of communication via the company intranet to determine that documented policies and procedures were in place to guide personnel in the entity's security and availability commitments and the associated system requirements and communicated to internal personnel via the company intranet.	No exceptions noted.
CC2.3: The responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties.			
CC2.3.1	The entity's security and availability commitments and the associated system requirements are documented and communicated to internal and external users via the following channels: • Customer contracts and nondisclosure agreements • Marketing materials and brochures	Inspected the customer contract and nondisclosure agreement templates as well as example marketing materials and brochures to determine that the entity's security and availability commitments and the associated system requirements were documented and communicated to internal and external users.	No exceptions noted.
CC2.3.2	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.	Inquired of the compliance manager regarding security awareness training to determine that employees were 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.	No exceptions noted.
		Inspected the training content and evidence of 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.
CC2.3.3	Employees are required to complete ethics training on an annual basis to understand their obligations and responsibilities to comply with the corporate code of business conduct and ethics.	Inquired of the compliance manager regarding ethics training to determine that employees were required to complete ethics training on an annual basis to understand their obligations and responsibilities to comply with the corporate code of business conduct and ethics.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the ethics training content and evidence of training completion for a sample of current employees to determine that each employee sampled completed ethics training during the review period.	No exceptions noted.
CC2.3.4	Documented policies and procedures are in place to guide personnel in the entity's security and availability commitments and the associated system requirements. The policies and procedures are communicated to internal personnel via the company intranet.	Inspected the security policies and employee handbook and evidence of communication via the company intranet to determine that documented policies and procedures were in place to guide personnel in the entity's security and availability commitments and the associated system requirements and communicated to internal personnel via the company intranet.	No exceptions noted.
CC2.4: Information necessary for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the security and availability of the system, is provided to personnel to carry out their responsibilities.			
CC2.4.1	The entity's security and availability commitments and the associated system requirements are documented and communicated to internal and external users via the following channels: • Customer contracts and nondisclosure agreements • Marketing materials and brochures	Inspected the customer contract and nondisclosure agreement templates as well as example marketing materials and brochures to determine that the entity's security and availability commitments and the associated system requirements were documented and communicated to internal and external users.	No exceptions noted.
CC2.4.2	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.	Inquired of the compliance manager regarding security awareness training to determine that employees were 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.	No exceptions noted.
		Inspected the training content and evidence of 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.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.4.3	Employees are required to complete ethics training on an annual basis to understand their obligations and responsibilities to comply with the corporate code of business conduct and ethics.	Inquired of the compliance manager regarding ethics training to determine that employees were required to complete ethics training on an annual basis to understand their obligations and responsibilities to comply with the corporate code of business conduct and ethics.	No exceptions noted.
		Inspected the ethics training content and evidence of training completion for a sample of current employees to determine that each employee sampled completed ethics training during the review period.	No exceptions noted.
CC2.4.4	Documented policies and procedures are in place to guide personnel in the entity's security and availability commitments and the associated system requirements. The policies and procedures are communicated to internal personnel via the company intranet.	Inspected the security policies and employee handbook and evidence of communication via the company intranet to determine that documented policies and procedures were in place to guide personnel in the entity's security and availability commitments and the associated system requirements and communicated to internal personnel via the company intranet.	No exceptions noted.
CC2.5: Internal and external users have been provided with information on how to report security and availability failures, incidents, concerns, and other complaints to appropriate personnel.			
CC2.5.1	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 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.
CC2.6: System changes that affect internal and external users' responsibilities or the entity's commitments and system requirements relevant to security and availability are communicated to those users in a timely manner.			
CC2.6.1	Issues regarding cabinet and cage installation requests, interconnection requests and trouble tickets are reviewed at an operations meeting on a bi-weekly basis.	Inquired of data center and operations personnel regarding the online customer support resource center to determine that issues regarding cabinet and cage installation requests, interconnection requests and trouble tickets were reviewed at an operations meeting on a bi-weekly basis.	No exceptions noted.
		Inspected the recurring calendar invitation and listing of invitees during the review period for the operations meetings to determine that operations meetings were held on a weekly basis.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.6.2	Organizational charts are in place to communicate the defined key areas of authority, responsibility and lines of reporting to personnel related to the design, development, implementation, operation, maintenance, and monitoring of the system. These charts are communicated to employees via the company intranet and updated as needed.	Inquired of the compliance manager regarding organizational management to determine that organizational charts were in place, communicated to employees, and updated as needed.	No exceptions noted.
		Inspected the company organizational charts to determine that organizational charts were in place to communicate the defined key areas of authority, responsibility and lines of reporting to personnel related to the design, development, implementation, operation, maintenance, and monitoring of the system and were updated as needed.	No exceptions noted.
		Inspected the organizational charts on the company intranet to determine that organizational charts were communicated to employees via the company intranet.	No exceptions noted.
CC2.6.3	Documented position descriptions are in place and updated as needed to communicate changes in roles and responsibilities.	Inspected the documented position descriptions for a sample of employment positions to determine that documented position descriptions were in place for each employment position sampled and were updated as needed to communicate changes in roles and responsibilities.	No exceptions noted.
CC3.0: Common Criteria Related to Risk Management and Design and Implementation of Controls			
CC3.1: The entity (1) identifies potential threats that could impair system security and availability commitments and system requirements (including threats arising from the use of vendors and other third parties providing goods and services, as well as threats arising from customer personnel and others with access to the system), (2) analyzes the significance of risks associated with the identified threats, (3) determines mitigation strategies for those risks (including implementation of controls, assessment and monitoring of vendors and other third parties providing goods or services, as well as their activities, and other mitigation strategies), (4) identifies and assesses changes (for example, environmental, regulatory, and technological changes and results of the assessment and monitoring of controls) that could significantly affect the system of internal control, and (5) reassesses, and revises, as necessary, risk assessments and mitigation strategies based on the identified changes.		
CC3.1.1	An inventory listing of infrastructure supporting the colocation services is maintained and reviewed on at least an annual basis.	Inquired of the compliance manager regarding the colocation facility assets to determine that an inventory listing of infrastructure supporting the colocation services was maintained and reviewed on at least an annual basis.	No exceptions noted.
		Inspected the infrastructure inventory listing to determine that the inventory listing of infrastructure supporting the colocation services was maintained and reviewed during the review period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.1.2	Documented policies and procedures are in place to guide personnel when performing the risk assessment process.	Inspected the risk assessment policy to determine that documented policies and procedures were in place to guide personnel when performing the risk assessment process.	No exceptions noted.
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 formal risk assessment was performed during the review period and that identified risks were formally documented for management review.	No exceptions noted.
CC3.1.4	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.	Inspected the most recent risk assessment documentation 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 during the review period.	No exceptions noted.
CC3.1.5	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.	Inspected example security updates and notifications during the review period 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.
CC3.2: The entity designs, develops, implements, and operates controls, including policies and procedures, to implement its risk mitigation strategy; reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities; and updates the controls, as necessary.			
CC3.2.1	Internal vulnerability assessments of the production environment are performed by IT personnel on a weekly basis.	Inspected the internal vulnerability assessment recurring schedule configurations and an example scan log generated during the review period to determine that internal vulnerability assessments of the production environment were performed by IT personnel on a weekly basis.	No exceptions noted.
CC3.2.2	Security incidents identified from internal vulnerability scans are documented and reviewed on an ad hoc basis by IT personnel.	Inquired of the information security manager regarding the security incident response process to determine that security incidents identified from internal vulnerability scans were documented and reviewed on an ad hoc basis by IT personnel.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected an example vulnerability assessment report completed during the review period to determine that security incidents identified from internal vulnerability scans were documented and reviewed on an ad hoc basis by IT personnel.	No exceptions noted.
CC3.2.3	Third party or internal security guards monitor physical security at the colocation facilities. Physical security at the DE2 colocation facility is monitored remotely.	Inquired of data center and operations personnel regarding security monitoring to determine that physical security at the DE2 colocation facility was monitored remotely.	No exceptions noted.
		Observed the security guards at each of the in-scope colocation facilities to determine that security guards monitored physical security at the applicable colocation facilities.	No exceptions noted.
		Inspected the security guard staffing schedule for each of the in-scope colocation facilities to determine that on-site third party or internal security guards monitored physical security at the applicable colocation facilities.	No exceptions noted.
CC3.2.4	Badge access control systems are in place to control access to and within the colocation facilities.	Observed the badge access control systems in place at each of the in-scope colocation facilities to determine that badge access control systems were in place to control access to and within the colocation facilities.	No exceptions noted.
		Inspected the badge access control system active user listing and example activity logs generated during the review period for each of the in-scope colocation facilities to determine that badge access control systems were in place to control access to and within the colocation facilities.	No exceptions noted.
CC3.2.5	NVR camera systems are in place to monitor activity to and throughout the colocation facilities.	Inquired of data center and operations personnel regarding the NVR camera systems to determine that NVR camera systems were utilized to monitor activity to and throughout the colocation facilities.	No exceptions noted.
		Observed the presence of multiple cameras at each of the in-scope colocation facilities to determine that NVR camera systems were in place.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC4.0: Common Criteria Related to Monitoring Controls			
CC4.1: The design and operating effectiveness of controls are periodically evaluated against the entity's commitments and system requirements as they relate to security and availability, and corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.			
CC4.1.1	Internal vulnerability assessments of the production environment are performed by IT personnel on a weekly basis.	Inspected the internal vulnerability assessment recurring schedule configurations and an example scan log generated during the review period to determine that internal vulnerability assessments of the production environment were performed by IT personnel on a weekly basis.	No exceptions noted.
CC4.1.2	Security incidents identified from internal vulnerability scans are documented and reviewed on an ad hoc basis by IT personnel.	Inquired of the information security manager regarding the security incident response process to determine that security incidents identified from internal vulnerability scans were documented and reviewed on an ad hoc basis by IT personnel.	No exceptions noted.
		Inspected an example vulnerability assessment report completed during the review period to determine that security incidents identified from internal vulnerability scans were documented and reviewed on an ad hoc basis by IT personnel.	No exceptions noted.
CC4.1.3	Security guards are alerted when an alarm panel within the colocation facilities is triggered.	Inquired of data center and operations personnel regarding monitoring of the alarm panels to determine that security guards were alerted when an alarm panel within the colocation facilities was triggered.	No exceptions noted.
		Observed example on-screen alerts generated at the security consoles at each of the in-scope colocation facilities during the review period to determine that security guards were alerted when an alarm panel was triggered.	No exceptions noted.
CC4.1.4	The badge access control system is configured to log predefined physical access related events and alert security personnel when certain events are identified.	Inspected example recent badge access control system logs and on-screen alerts generated during the review period for each of the in-scope colocation facilities to determine that the badge access control system was configured to log predefined physical access related events and alert security personnel when certain events were identified.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC4.1.5	Historical activity logs from the badge access control system are retained for a minimum of 90 days.	Inspected historical activity logs generated during the review period for each of the in-scope colocation facilities to determine that historical activity logs from the badge access control system were retained for a minimum of 90 days.	No exceptions noted.
CC4.1.6	NVR images are retained for a minimum of 90 days.	Inquired of data center and operations personnel regarding NVR archives to determine that NVR images were retained for a minimum of 90 days.	No exceptions noted.
		Inspected historical NVR images archived during the review period for each of the in-scope colocation facilities to determine that NVR images were retained for a minimum of 90 days.	No exceptions noted.
CC4.1.7	The building automation systems are configured to alert operations personnel when predefined thresholds are exceeded or alarms are triggered on monitored devices.	Inspected the alerting configurations and example e-mail alerts generated during the review period for each of the in-scope colocation facilities to determine that the building automation systems were configured to alert operations personnel when predefined thresholds were exceeded or alarms were triggered on monitored systems.	No exceptions noted.
CC4.1.8	Documented escalation procedures are in place to guide employees in reporting, acting upon, and resolving reported events.	Inspected the escalation procedures to determine that documented escalation procedures were in place to guide employees in reporting, acting upon, and resolving reported events.	No exceptions noted.
CC5.0: Common Criteria Related to Logical and Physical Access Controls			
CC5.1: Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to security and availability.			
CC5.1.1	Documented standard build procedures are utilized for installation and maintenance of production servers and infrastructure.	Inspected the standard build procedures to determine that documented standard build procedures were utilized for installation and maintenance of production servers.	No exceptions noted.
CC5.1.2	User access reviews of the network domain are performed on a semi-annual basis to help ensure that access to data is restricted and provides for appropriate segregation of duties.	Inspected the most recently completed access reviews to determine that user access reviews of the network domain were performed on a semi-annual basis during the review period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.1.3	The in-scope systems are configured to authenticate users with a user account and enforce predefined user account and minimum password requirements.	Inspected the user account listings and minimum password requirements for a sample of in-scope systems to determine that the following in-scope systems sampled were configured to authenticate users with a user account and enforce predefined user account and minimum password requirements: • Network domain • Jump servers • Production servers • Databases • Badge access control application • Firewalls • VPN	No exceptions noted.
CC5.1.4	TLS encrypted VPNs are required for remote access to production and inherit predefined user account and minimum password requirements from the network domain.	Inspected the VPN encryption and authentication configurations to determine that TLS encrypted VPNs were required for remote access and that predefined user account and minimum password requirements were inherited from the network domain.	No exceptions noted.
CC5.1.5	Predefined security groups are utilized to assign role-based access privileges and segregate access to data to the in-scope systems.	Inspected the user account listings for a sample of in-scope systems to determine that predefined security groups were utilized to assign role-based access privileges and segregate access to data to the following in-scope system sampled: • Network domain • Jump servers • Production servers • Databases • Badge access control application • Firewalls • VPN	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.1.6	Administrative access privileges to the in-scope systems are restricted to user accounts accessible by authorized personnel.	Inspected the administrator user account listings for a sample of in-scope systems with the assistance of the systems manager to determine that administrative access privileges to the following in-scope systems sampled were restricted to user accounts accessible by authorized personnel: • Network domain • Jump servers • Production servers • Databases • Badge access control application • Firewalls • VPN	No exceptions noted.
CC5.1.7	Privileged user access reviews of the network domain are performed on a semi-annual basis to help ensure that access to data is restricted and authorized.	Inspected the most recently completed access reviews to determine that privileged user access reviews of the network domain were performed on a semi-annual basis during the review period.	No exceptions noted.
CC5.1.8	Logical access requests for internal users are documented on an access request ticket and require manager approval.	Inspected user access request tickets for a sample of internal users provided logical access during the review period to determine that logical access requests were documented on an access request ticket and were approved by a manager for each internal user sampled.	No exceptions noted.
CC5.2: New internal and external users, whose access is administered by the entity, are registered and authorized prior to being issued system credentials and granted the ability to access the system to meet the entity's commitments and system requirements as they relate to security and availability. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			
CC5.2.1	Logical access requests for internal users are documented on an access request ticket and require manager approval.	Inspected user access request tickets for a sample of internal users provided logical access during the review period to determine that logical access requests were documented on an access request ticket and were approved by a manager for each internal user sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.2.2	A termination ticket is completed and systems access is revoked for employees as a component of the employee termination process.	Inspected the termination ticket and user account listings for a sample of in-scope systems and employees terminated during the review period to determine that a termination ticket was completed and access was revoked to each of the following in-scope systems sampled for each terminated employee sampled: • Network domain • Jump servers • Production servers • Databases • Badge access control application • Firewalls • VPN	No exceptions noted.
CC5.3: Internal and external users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data) to meet the entity's commitments and system requirements as they relate to security and availability.			
CC5.3.1	The in-scope systems are configured to authenticate users with a user account and enforce predefined user account and minimum password requirements.	Inspected the user account listings and minimum password requirements for a sample of in-scope systems to determine that the following in-scope systems sampled were configured to authenticate users with a user account and enforce predefined user account and minimum password requirements: • Network domain • Jump servers • Production servers • Databases • Badge access control application • Firewalls • VPN	No exceptions noted.
CC5.3.2	TLS encrypted VPNs are required for remote access to production and inherit predefined user account and minimum password requirements from the network domain.	Inspected the VPN encryption and authentication configurations to determine that TLS encrypted VPNs were required for remote access and that predefined user account and minimum password requirements were inherited from the network domain.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.4: Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to meet the entity's commitments and system requirements as they relate to security and availability.			
CC5.4.1	Logical access requests for internal users are documented on an access request ticket and require manager approval.	Inspected user access request tickets for a sample of internal users provided logical access during the review period to determine that logical access requests were documented on an access request ticket and were approved by a manager for each internal user sampled.	No exceptions noted.
CC5.4.2	User access reviews of the network domain are performed on a semi-annual basis to help ensure that access to data is restricted and provides for appropriate segregation of duties.	Inspected the most recently completed access reviews to determine that user access reviews of the network domain were performed on a semi-annual basis during the review period.	No exceptions noted.
CC5.4.3	A termination ticket is completed and systems access is revoked for employees as a component of the employee termination process.	Inspected the termination ticket and user account listings for a sample of in-scope systems and employees terminated during the review period to determine that a termination ticket was completed and access was revoked to each of the following in-scope systems sampled for each terminated employee sampled: • Network domain • Jump servers • Production servers • Databases • Badge access control application • Firewalls • VPN	No exceptions noted.
CC5.5: Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations, as well as sensitive system components within those locations) is restricted to authorized personnel to meet the entity's commitments and system requirements as they relate to security and availability.			
CC5.5.1	A security procedures manual is in place to guide personnel in carrying out the following security procedures and related activities: • Badge access control system • Visitor management • Deliveries • Property removal • Support services	Inspected the security procedures manual to determine that a security procedures manual was documented to guide personnel in carrying out the following security procedures and related activities: • Badge access control system • Visitor management • Deliveries • Property removal • Support services	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.5.2	Third party or internal security guards monitor physical security at the colocation facilities. Physical security at the DE2 colocation facility is monitored remotely.	Inquired of data center and operations personnel regarding security monitoring to determine that physical security at the DE2 colocation facility was monitored remotely.	No exceptions noted.
		Observed the security guards at each of the in-scope colocation facilities to determine that security guards monitored physical security at the applicable colocation facilities.	No exceptions noted.
		Inspected the security guard staffing schedule for each of the in-scope colocation facilities to determine that on-site third party or internal security guards monitored physical security at the applicable colocation facilities.	No exceptions noted.
CC5.5.3	Security guards are alerted when an alarm panel within the colocation facilities is triggered.	Inquired of data center and operations personnel regarding monitoring of the alarm panels to determine that security guards were alerted when an alarm panel within the colocation facilities was triggered.	No exceptions noted.
		Observed example on-screen alerts generated at the security consoles at each of the in-scope colocation facilities during the review period to determine that security guards were alerted when an alarm panel was triggered.	No exceptions noted.
CC5.5.4	Badge access control systems are in place to control access to and within the colocation facilities.	Observed the badge access control systems in place at each of the in-scope colocation facilities to determine that badge access control systems were in place to control access to and within the colocation facilities.	No exceptions noted.
		Inspected the badge access control system active user listing and example activity logs generated during the review period for each of the in-scope colocation facilities to determine that badge access control systems were in place to control access to and within the colocation facilities.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.5.5	The badge access control system is configured to log predefined physical access related events and alert security personnel when certain events are identified.	Inspected example recent badge access control system logs and on-screen alerts generated during the review period for each of the in-scope colocation facilities to determine that the badge access control system was configured to log predefined physical access related events and alert security personnel when certain events were identified.	No exceptions noted.
CC5.5.6	Historical activity logs from the badge access control system are retained for a minimum of 90 days.	Inspected historical activity logs generated during the review period for each of the in-scope colocation facilities to determine that historical activity logs from the badge access control system were retained for a minimum of 90 days.	No exceptions noted.
CC5.5.7	Visitors are required to provide photo identification, to be logged in the badge access control systems and/or sign a visitor log, and are issued a temporary badge for use while within the colocation facilities.	Observed the visitor entrance procedures at each of the in-scope colocation facilities to determine that visitors were required to provide photo identification to be logged in the badge access control systems and/or sign a visitor log and were issued a temporary badge for use while within the colocation facilities.	No exceptions noted.
		Inspected the visitor logs for each of the in-scope colocation facilities for a sample of dates during the review period to determine that visitors were logged for each date sampled.	No exceptions noted.
CC5.5.8	Historical visitor logs are retained for a minimum of 90 days.	Inspected historical visitor logs during the review period for each of the in-scope colocation facilities to determine that historical visitor logs were retained for a minimum of 90 days.	No exceptions noted.
CC5.5.9	Visitors are required to be escorted by authorized personnel while within the colocation facilities.	Observed the visitor entrance procedures at each of the in-scope colocation facilities to determine that visitors were required to be escorted by authorized personnel while within the colocation facilities.	No exceptions noted.
CC5.5.10	NVR camera systems are in place to monitor activity to and throughout the colocation facilities.	Inquired of data center and operations personnel regarding the NVR camera systems to determine that NVR camera systems were utilized to monitor activity to and throughout the colocation facilities.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Observed the presence of multiple cameras at each of the in-scope colocation facilities to determine that NVR camera systems were in place.	No exceptions noted.
CC5.5.11	NVR images are retained for a minimum of 90 days.	Inquired of data center and operations personnel regarding NVR archives to determine that NVR images were retained for a minimum of 90 days.	No exceptions noted.
		Inspected historical NVR images archived during the review period for each of the in-scope colocation facilities to determine that NVR images were retained for a minimum of 90 days.	No exceptions noted.
CC5.5.12	Physical access requests for external users are documented on an access request ticket and are required to be submitted to facilities security personnel for processing.	Inspected user access request tickets for a sample of external users provided physical access to each of the in-scope colocation facilities during the review period to determine that physical access requests were documented on an access request ticket and submitted to facilities security personnel for processing for each external user sampled.	No exceptions noted.
CC5.5.13	Physical access requests for internal users are documented on an access request ticket and require manager approval.	Inspected user access request tickets for a sample of internal users provided physical access to each of the in-scope colocation facilities during the review period to determine that physical access requests were documented on an access request ticket and were approved by a manager for each internal user sampled.	No exceptions noted.
CC5.5.14	Physical access reviews are performed on a semi-annual basis to help ensure that access to the data center facilities is restricted.	Inspected the most recently completed badge access control system physical access review for each of the in-scope colocation facilities to determine that a physical access review was performed on a semi-annual basis during the review period.	No exceptions noted.
CC5.5.15	A termination ticket is completed and physical access is revoked for employees as a component of the employee termination process.	Inspected the termination ticket and badge access control system listing for each of the in-scope colocation facilities for a sample of employees terminated during the review period to determine that a termination ticket was completed and physical access was revoked for each terminated employee sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.6: Logical access security measures have been implemented to protect against security and availability threats from sources outside the boundaries of the system to meet the entity's commitments and system requirements.			
CC5.6.1	A firewall system is in place to filter unauthorized inbound network traffic from the Internet.	Inspected the network diagram and the firewall ruleset for the in-scope firewalls to determine that a firewall system was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
CC5.6.2	The firewall system is configured for high availability to provide failover firewall services in the event of a primary firewall failure.	Inspected the network diagram and firewall failover configurations for the in-scope firewalls to determine that the firewall system was configured for high availability to provide failover firewall services in the event of a primary firewall failure.	No exceptions noted.
CC5.6.3	TLS encrypted VPNs are required for remote access to production and inherit predefined user account and minimum password requirements from the network domain.	Inspected the VPN encryption and authentication configurations to determine that TLS encrypted VPNs were required for remote access and that predefined user account and minimum password requirements were inherited from the network domain.	No exceptions noted.
CC5.6.4	Internal vulnerability assessments of the production environment are performed by IT personnel on a weekly basis.	Inspected the internal vulnerability assessment recurring schedule configurations and an example scan log generated during the review period to determine that internal vulnerability assessments of the production environment were performed by IT personnel on a weekly basis.	No exceptions noted.
CC5.6.5	Security incidents identified from internal vulnerability scans are documented and reviewed on an ad hoc basis by IT personnel.	Inquired of the information security manager regarding the security incident response process to determine that security incidents identified from internal vulnerability scans were documented and reviewed on an ad hoc basis by IT personnel.	No exceptions noted.
		Inspected an example vulnerability assessment report completed during the review period to determine that security incidents identified from internal vulnerability scans were documented and reviewed on an ad hoc basis by IT personnel.	No exceptions noted.
CC5.6.6	Firewall rules are reviewed on a quarterly basis to help ensure that only necessary connections are configured within the rulesets.	Inquired of the senior network engineer and information security architect regarding firewall ruleset reviews to determine that firewall rules were reviewed on a quarterly basis to ensure that only necessary connections were configured within the rulesets.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the firewall ruleset reviews for a sample of quarters during the review period to determine that firewall rules were reviewed for each quarter sampled.	No exceptions noted.
CC5.6.7	Firewall ruleset changes are required to be documented within the automated ticketing system and approved prior to implementation.	Inspected the ticketing documentation for a sample of firewall ruleset changes implemented during the review period to determine that each firewall ruleset change sampled was documented within the automated ticketing system and approved prior to implementation.	No exceptions noted.
CC5.7: The transmission, movement, and removal of information is restricted to authorized internal and external users and processes and is protected during transmission, movement, or removal, enabling the entity to meet its commitments and system requirements as they relate to security and availability.			
CC5.7.1	TLS encrypted VPNs are required for remote access to production and inherit predefined user account and minimum password requirements from the network domain.	Inspected the VPN encryption and authentication configurations to determine that TLS encrypted VPNs were required for remote access and that predefined user account and minimum password requirements were inherited from the network domain.	No exceptions noted.
CC5.7.2	Documented policies and 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 encryption policies to determine that documented policies and 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.
CC5.7.3	Transaction log backup files from the primary production database are log shipped to a secondary, standby server at a separate geographic location every 15 minutes over a private connection.	Inquired of the compliance manager regarding log shipping to determine that transaction log backup files from the primary production database were log shipped to a secondary, standby server at separate geographic location every 15 minutes over a private connection.	No exceptions noted.
		Inspected the log shipping configurations and example job history restore logs generated during the review period to determine that transaction log backup files from the primary production database were log shipped to a secondary, standby server at a separate geographic location every 15 minutes.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.8: Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's commitments and system requirements as they relate to security and availability.			
CC5.8.1	A central antivirus server is configured with antivirus software to protect registered production Windows servers supporting the badge access control system and workstations with the following configurations: • Scan for updates to antivirus definitions and update registered clients on a daily basis • Scan registered clients on a weekly basis	Inspected the enterprise antivirus software configurations and registered client listing to determine that enterprise antivirus software was installed on production Windows servers supporting the badge access control system and workstations and configured as follows: • Scan for updates to antivirus definitions and update registered clients on a daily basis • Scan registered clients on a weekly basis	No exceptions noted.
CC6.0: Common Criteria Related to System Operations			
CC6.1: Vulnerabilities of system components to security and availability breaches and incidents due to malicious acts, natural disasters, or errors are identified, monitored, and evaluated, and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities to meet the entity's commitments and system requirements as they relate to security and availability.			
CC6.1.1	Internal vulnerability assessments of the production environment are performed by IT personnel on a weekly basis.	Inspected the internal vulnerability assessment recurring schedule configurations and an example scan log generated during the review period to determine that internal vulnerability assessments of the production environment were performed by IT personnel on a weekly basis.	No exceptions noted.
CC6.1.2	Security incidents identified from internal vulnerability scans are documented and reviewed on an ad hoc basis by IT personnel.	Inquired of the information security manager regarding the security incident response process to determine that security incidents identified from internal vulnerability scans were documented and reviewed on an ad hoc basis by IT personnel.	No exceptions noted.
		Inspected an example vulnerability assessment report completed during the review period to determine that security incidents identified from internal vulnerability scans were documented and reviewed on an ad hoc basis by IT personnel.	No exceptions noted.
CC6.1.3	Security guards are alerted when an alarm panel within the colocation facilities is triggered.	Inquired of data center and operations personnel regarding monitoring of the alarm panels to determine that security guards were alerted when an alarm panel within the colocation facilities was triggered.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Observed example on-screen alerts generated at the security consoles at each of the in-scope colocation facilities during the review period to determine that security guards were alerted when an alarm panel was triggered.	No exceptions noted.
CC6.1.4	The badge access control system is configured to log predefined physical access related events and alert security personnel when certain events are identified.	Inspected example recent badge access control system logs and on-screen alerts generated during the review period for each of the in-scope colocation facilities to determine that the badge access control system was configured to log predefined physical access related events and alert security personnel when certain events were identified.	No exceptions noted.
CC6.1.5	The building automation systems are configured to alert operations personnel when predefined thresholds are exceeded or alarms are triggered on monitored devices.	Inspected the alerting configurations and example e-mail alerts generated during the review period for each of the in-scope colocation facilities to determine that the building automation systems were configured to alert operations personnel when predefined thresholds were exceeded or alarms were triggered on monitored systems.	No exceptions noted.
CC6.1.6	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 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.
CC6.1.7	Automated backup systems are in place to perform scheduled backups of production servers supporting the badge access control system at predefined times.	Inspected the backup schedule configurations and example backup logs generated during the review period for a sample of production servers supporting the badge access control system to determine that automated backup systems were in place to perform scheduled backups of each server sampled at predefined times.	No exceptions noted.
CC6.1.8	Automated backup systems are in place to perform scheduled differential backups of production servers supporting the badge access control system on a daily basis.	Inspected the backup schedule configurations and example backup logs generated during the review period for a sample of production servers supporting the badge access control system to determine that automated backup systems were in place to perform scheduled differential backups of each server sampled on a daily basis.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.1.9	Automated backup systems are in place to perform scheduled full backups of production servers supporting the badge access control system on a weekly basis.	Inspected the backup schedule configurations and example backup logs generated during the review period for a sample of production servers supporting the badge access control system to determine that automated backup systems were in place to perform scheduled full backups of each server sampled on a weekly basis.	No exceptions noted.
CC6.2: Security and availability incidents, including logical and physical security breaches, failures, and identified vulnerabilities, are identified and reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's commitments and system requirements.			
CC6.2.1	Documented escalation procedures are in place to guide employees in reporting, acting upon, and resolving reported events.	Inspected the escalation procedures to determine that documented escalation procedures were in place to guide employees in reporting, acting upon, and resolving reported events.	No exceptions noted.
CC6.2.2	Management meetings are held on at least a quarterly basis to discuss incidents and corrective measures to help ensure that incidents are resolved.	Inspected the recurring management meeting calendar invite and example meeting minutes during the review period to determine that management meetings were held to discuss incidents and corrective measures to ensure that incidents were resolved on at least a quarterly basis.	No exceptions noted.
CC6.2.3	Help desk and operations personnel utilize an automated ticketing system to document security violations, responses, and resolution.	Inspected a listing of the closed security incident tickets during the review period and the ticket detail for an example security incident closed during the review period to determine that an automated ticketing system was utilized to document security violations, responses, and resolution.	No exceptions noted.
CC6.2.4	Documented policies and procedures are in place that address remedial actions for lack of compliance with policies and procedures.	Inspected the employee handbook to determine that documented policies and procedures were in place that addressed remedial actions for lack of compliance with policies and procedures.	No exceptions noted.
CC6.2.5	Incidents requiring a change to the system follow the standard change control process.	Inspected the ticketing documentation for an example security incident requiring a change during the review period to determine that incidents requiring a change to the system followed the standard change control process.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.0: Common Criteria Related to Change Management			
CC7.1: The entity's commitments and system requirements, as they relate to security and availability, are addressed during the system development lifecycle, including the authorization, design, acquisition, implementation, configuration, testing, modification, approval, and maintenance of system components.			
CC7.1.1	Documented change management policies and procedures are in place to guide personnel in the request, documentation, testing, and approval of system changes.	Inspected the change management and software development policy to determine that documented change management policies were in place to guide personnel in the request, documentation, testing, and approval of system changes.	No exceptions noted.
CC7.1.2	An automated ticketing system is utilized to log and track operating system patches and upgrades made to the production servers supporting the badge access control system and application updates made to the badge access control system.	Inspected the automated ticketing system dashboard to determine that an automated ticketing system was utilized to log and track operating system patches and upgrades made to the production servers supporting the badge access control system and application updates made to the badge access control system.	No exceptions noted.
CC7.1.3	Operating system patches and upgrades made to production servers supporting the badge access control system are authorized, tested, and approved prior to implementation.	Inquired of the manager of systems and help desk to determine that operating system patches and upgrades made to production servers supporting the badge access control system were authorized, tested, and approved prior to implementation.	No exceptions noted.
		Inspected the ticketing documentation for a sample of operating system patches / upgrades made to the production servers supporting the badge access control system during the review period to determine that each patch / upgrade sampled was authorized, tested, and approved prior to implementation.	No exceptions noted.
CC7.1.4	Application updates made to the badge access control system are authorized, tested, and approved prior to implementation. Additionally, a post-implementation review is performed to help ensure proper functioning of the application in the production environment.	Inspected the listing of application updates made to the badge access control system during the review period and determined that no application updates occurred during the review period; therefore, no testing of operating effectiveness was performed.	

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.2: Infrastructure, data, software, and policies and procedures are updated as necessary to remain consistent with the entity's commitments and system requirements as they relate to security and availability.			
CC7.2.1	A formal risk assessment is performed on an annual basis. Risks that are identified and require changes to the system are documented in the automated ticketing system.	Inspected the most recent risk assessment documentation and the ticketing documentation for an example change implemented during the review period to determine that a formal risk assessment was performed during the review period and that risks that were identified and required changes to the system were documented in the automated ticketing system.	No exceptions noted.
CC7.2.2	Management meetings are held on at least a quarterly basis to discuss incidents and corrective measures to help ensure that incidents are resolved.	Inspected the recurring management meeting calendar invite and example meeting minutes during the review period to determine that management meetings were held to discuss incidents and corrective measures to ensure that incidents were resolved on at least a quarterly basis.	No exceptions noted.
CC7.3: Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and are monitored to meet the entity's commitments and system requirements as they relate to security and availability.			
CC7.3.1	Incidents requiring a change to the system follow the standard change control process.	Inspected the ticketing documentation for an example security incident requiring a change during the review period to determine that incidents requiring a change to the system followed the standard change control process.	No exceptions noted.
CC7.4: Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented to meet the entity's security and availability commitments and system requirements.			
CC7.4.1	Documented change management policies and procedures are in place to guide personnel in the request, documentation, testing, and approval of system changes.	Inspected the change management and software development policy to determine that documented change management policies were in place to guide personnel in the request, documentation, testing, and approval of system changes.	No exceptions noted.
CC7.4.2	Operating system patches and upgrades made to production servers supporting the badge access control system are authorized, tested, and approved prior to implementation.	Inquired of the manager of systems and help desk to determine that operating system patches and upgrades made to production servers supporting the badge access control system were authorized, tested, and approved prior to implementation.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the ticketing documentation for a sample of operating system patches / upgrades made to the production servers supporting the badge access control system during the review period to determine that each patch / upgrade sampled was authorized, tested, and approved prior to implementation.	No exceptions noted.
CC7.4.3	Application updates made to the badge access control system are authorized, tested, and approved prior to implementation. Additionally, a post-implementation review is performed to help ensure proper functioning of the application in the production environment.	Inspected the listing of application updates made to the badge access control system during the review period and determined that no application updates occurred during the review period; therefore, no testing of operating effectiveness was performed.	
CC7.4.4	The ability to promote application updates and operating system patches and upgrades into the production environment is restricted to user accounts accessible by authorized personnel.	Inspected administrator user account listings for a sample of production servers supporting the badge access control system with the assistance of the senior systems engineer to determine that the ability to promote application updates and operating system patches and upgrades into the production environment was restricted to user accounts accessible by authorized personnel for each server sampled.	No exceptions noted.
CC7.4.5	Automated backup systems are in place to perform scheduled backups of production servers supporting the badge access control system at predefined times to allow for rollback of changes when changes impair system operation.	Inspected the backup schedule configurations and example backup logs generated during the review period for a sample of production servers supporting the badge access control system to determine that automated backup systems were in place to perform scheduled backups of each server sampled at predefined times to allow for rollback of changes when changes impaired system operation.	No exceptions noted.

AVAILABILITY PRINCIPLE AND CRITERIA TABLE

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.1: Current processing capacity and usage are maintained, monitored, and evaluated to manage capacity demand and to enable the implementation of additional capacity to help meet the entity's availability commitments and system requirements.			
A1.1.1	Backup power infrastructure, including UPS systems and generators, are in place to provide power to the colocation facilities in the event of a primary power outage.	Inquired of data center and operations personnel regarding data center power to determine that backup power infrastructure was in place to provide power to the colocation facilities in the event of a primary power outage.	No exceptions noted.
		Observed the backup power infrastructure at each of the in-scope colocation facilities to determine that backup power infrastructure was in place to provide power to the colocation facilities in the event of a primary power outage.	No exceptions noted.
A1.1.2	Redundant UPS systems are in place to provide temporary power in the event of a power failure and to mitigate the risk of power surges impacting infrastructure in the colocation facilities.	Inquired of data center and operations personnel regarding the UPS systems to determine that redundant UPS systems were in place to provide temporary power in the event of a power failure and to mitigate the risk of power surges impacting infrastructure in the colocation facilities.	No exceptions noted.
		Observed the presence of multiple UPS systems at each of the in-scope colocation facilities to determine that multiple UPS systems were in place at the colocation facilities.	No exceptions noted.
A1.1.3	Multiple air conditioners and/or handlers are in place to cool the colocation facilities and provide redundancy.	Inquired of data center and operations personnel regarding data center cooling to determine that multiple air conditioners and/or handlers were in place to cool the colocation facilities and provide redundancy.	No exceptions noted.
		Observed the presence of multiple air conditioners and/or handlers and chiller tanks, as applicable, at each of the in-scope colocation facilities to determine that multiple air conditioners and/or handlers and water chillers were in place.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.1.4	Power supply equipment owned and managed by CoreSite is monitored by building automation systems.	Inspected the building automation system configurations for each of the in-scope colocation facilities to determine that power supply equipment owned and managed by CoreSite was monitored by building automation systems.	No exceptions noted.
A1.1.5	The building automation systems are configured to monitor environmental conditions, including temperature and humidity levels, at the colocation facilities.	Inspected the building automation system configurations for each of the in-scope colocation facilities to determine that the building automation systems were configured to monitor environmental conditions, including temperature and humidity levels.	No exceptions noted.
A1.1.6	The building automation systems are configured to alert operations personnel when predefined thresholds are exceeded or alarms are triggered on monitored devices.	Inspected the alerting configurations and example e-mail alerts generated during the review period for each of the in-scope colocation facilities to determine that the building automation systems were configured to alert operations personnel when predefined thresholds were exceeded or alarms were triggered on monitored systems.	No exceptions noted.
A1.1.7	Members of the capacity planning team utilize automated monitoring tools and reports to monitor the power and utilization levels of the colocation facilities and supporting infrastructure on a real-time basis.	Inquired of the senior manager of capacity and inventory management regarding the monitoring of utilization thresholds to determine that members of the capacity planning team utilized automated monitoring tools and reports to monitor the power and utilization levels of the colocation facilities and supporting infrastructure on a real-time basis.	No exceptions noted.
		Inspected the automated monitoring tool configurations and example reports generated during the review period to determine that members of the capacity planning team utilized automated monitoring tools and reports to monitor the power and utilization levels of the colocation facilities and supporting infrastructure on a real-time basis.	No exceptions noted.
A1.1.8	Management meetings are held on a quarterly basis to review availability trends and availability forecasts as compared to system commitments.	Inspected the capacity review meeting minutes for a sample of quarters during the review period to determine that management meetings were held to review availability trends and availability forecasts as compared to system commitments for each quarter sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.1.9	An enterprise monitoring application is configured to monitor the capacity levels of the production servers supporting the badge access control system and alert IT personnel when predefined thresholds are met.	Inspected the enterprise monitoring application configurations and an example e-mail notification generated during the review period to determine that an enterprise monitoring application was configured to monitor the capacity levels of the production servers supporting the badge access control system and alert IT personnel when predefined thresholds were met.	No exceptions noted.
A1.2: Environmental protections, software, data backup processes, and recovery infrastructure are authorized, designed, developed, implemented, operated, approved, maintained, and monitored to meet the entity's availability commitments and system requirements.			
A1.2.1	Backup power infrastructure, including UPS systems and generators, are in place to provide power to the colocation facilities in the event of a primary power outage.	Inquired of data center and operations personnel regarding data center power to determine that backup power infrastructure was in place to provide power to the colocation facilities in the event of a primary power outage.	No exceptions noted.
		Observed the backup power infrastructure at each of the in-scope colocation facilities to determine that backup power infrastructure was in place to provide power to the colocation facilities in the event of a primary power outage.	No exceptions noted.
A1.2.2	Redundant UPS systems are in place to provide temporary power in the event of a power failure and to mitigate the risk of power surges impacting infrastructure in the colocation facilities.	Inquired of data center and operations personnel regarding the UPS systems to determine that redundant UPS systems were in place to provide temporary power in the event of a power failure and to mitigate the risk of power surges impacting infrastructure in the colocation facilities.	No exceptions noted.
		Observed the presence of multiple UPS systems at each of the in-scope colocation facilities to determine that multiple UPS systems were in place at the colocation facilities.	No exceptions noted.
A1.2.3	Multiple air conditioners and/or handlers are in place to cool the colocation facilities and provide redundancy.	Inquired of data center and operations personnel regarding data center cooling to determine that multiple air conditioners and/or handlers were in place to cool the colocation facilities and provide redundancy.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Observed the presence of multiple air conditioners and/or handlers and chiller tanks, as applicable, at each of the in-scope colocation facilities to determine that multiple air conditioners and/or handlers and water chillers were in place.	No exceptions noted.
A1.2.4	The colocation facilities are equipped with fire detection and suppression controls that include the following: • Audible and visual fire alarms • Dry-pipe water sprinklers or FM-200 fire suppression systems • Fire and smoke detectors • Hand-held fire extinguishers	Observed the fire detection and suppression equipment during the review period to determine that the colocation facilities were equipped with fire detection and suppression controls that included the following: • Audible and visual fire alarms • Dry-pipe water sprinklers or FM-200 fire suppression systems • Fire and smoke detectors • Hand-held fire extinguishers	No exceptions noted.
A1.2.5	Management ensures that third party vendors inspect the UPS systems on at least an annual basis to help ensure proper functioning.	Inquired of data center and operations personnel regarding the UPS systems to determine that third party vendors inspected the UPS systems on at least an annual basis to ensure proper functioning.	No exceptions noted.
		Inspected the third party vendor service agreement and the most recent preventative maintenance inspection reports to determine that third party vendors inspected and maintained the UPS systems during the review period.	No exceptions noted.
A1.2.6	Internal personnel inspect the generators owned and managed by CoreSite on a monthly basis to help ensure proper functioning. If the generator has run under load due to an event or third party inspection, the monthly exercise will not be required again for another 30 days from that event.	Inquired of data center and operations personnel regarding generator inspections to determine that internal personnel inspected the generators on a monthly basis to ensure proper functioning.	No exceptions noted.
		Inspected the generator inspection logs for a sample of months during the review period to determine that internal personnel inspected the generators owned and managed by CoreSite for each month sampled.	No exceptions noted.
A1.2.7	Management ensures that third party vendors inspect the generators on a quarterly basis to help ensure proper functioning.	Inquired of data center and operations personnel regarding the generator inspections to determine that third party vendors inspected the generators on a quarterly basis to ensure proper functioning.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the third party vendor service agreements and preventative maintenance inspection reports for a sample of quarters during the review period to determine that third party vendors inspected the generators for each quarter sampled.	No exceptions noted.
A1.2.8	Management ensures that third party vendors or internal personnel inspect cooling equipment on a quarterly basis to help ensure proper functioning.	Inquired of data center and operations personnel regarding the cooling equipment to determine that third party vendors or internal personnel inspected cooling equipment on a quarterly basis to ensure proper functioning.	No exceptions noted.
		Inspected the third party vendor service agreement and the preventive maintenance inspection rereports for a sample of quarters during the review period to determine that third party vendors or internal personnel inspected the cooling equipment for each quarter sampled.	No exceptions noted.
A1.2.9	Management ensures that third party vendors inspect the fire detection and suppression equipment on at least an annual basis to help ensure proper functioning.	Inspected the most recent fire detection and suppression equipment preventative maintenance inspection reports to determine that third party vendors inspected the fire detection and suppression equipment during the review period.	No exceptions noted.
A1.2.10	Servers are maintained in racks to facilitate cooling and protect equipment from localized flooding.	Observed the placement of server racks at each of the colocation facilities to determine that servers were maintained in racks to facilitate cooling and protect equipment from localized flooding.	No exceptions noted.
A1.2.11	Power supply equipment owned and managed by CoreSite is monitored by building automation systems.	Inspected the building automation system configurations for each of the in-scope colocation facilities to determine that power supply equipment owned and managed by CoreSite was monitored by building automation systems.	No exceptions noted.
A1.2.12	The building automation systems are configured to monitor environmental conditions, including temperature and humidity levels, at the colocation facilities.	Inspected the building automation system configurations for each of the in-scope colocation facilities to determine that the building automation systems were configured to monitor environmental conditions, including temperature and humidity levels.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.2.13	The building automation systems are configured to alert operations personnel when predefined thresholds are exceeded or alarms are triggered on monitored devices.	Inspected the alerting configurations and example e-mail alerts generated during the review period to determine that the building automation systems were configured to alert operations personnel when predefined thresholds were exceeded or alarms were triggered on monitored systems.	No exceptions noted.
A1.2.14	Automated backup systems are in place to perform scheduled backups of production servers supporting the badge access control system at predefined times.	Inspected the backup schedule configurations and example backup logs generated during the review period for a sample of production servers supporting the badge access control system to determine that automated backup systems were in place to perform scheduled backups of each server sampled at predefined times.	No exceptions noted.
A1.2.15	Automated backup systems are in place to perform scheduled incremental backups of production servers supporting the badge access control system on a daily basis.	Inspected the backup schedule configurations and example backup logs generated during the review period for a sample of production servers supporting the badge access control system to determine that automated backup systems were in place to perform scheduled incremental backups of each server sampled on a daily basis.	No exceptions noted.
A1.2.16	Automated backup systems are in place to perform scheduled full backups of production servers supporting the badge access control system on a weekly basis.	Inspected the backup schedule configurations and example backup logs generated during the review period for a sample of production servers supporting the badge access control system to determine that automated backup systems were in place to perform scheduled full backups of each server sampled on a weekly basis.	No exceptions noted.
A1.2.17	The automated backup systems are configured to send alert notifications to IT personnel regarding backup job completion status.	Inspected the backup notification configurations and example alert notifications generated during the review period for a sample of production servers supporting the badge access control system to determine that the automated backup systems were configured to send alert notifications to IT personnel regarding backup job completion status for each server sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.2.18	Transaction log backup files from the primary production database are log shipped to a secondary, standby server at a separate geographic location every 15 minutes over a private connection.	Inquired of the compliance manager regarding log shipping to determine that transaction log backup files from the primary production database were log shipped to a secondary, standby server at separate geographic location every 15 minutes over a private connection.	No exceptions noted.
		Inspected the log shipping configurations and example recent job history restore logs for the primary production database to determine that transaction log backup files from the primary production database were log shipped to a secondary, standby server at a separate geographic location every 15 minutes.	No exceptions noted.
A1.2.19	IT personnel are notified upon failures of the log shipping process via e-mail.	Inspected the log shipping notification configurations and an example e-mail alert notification generated during the review period to determine that IT personnel were notified upon failures of the log shipping process via e-mail.	No exceptions noted.
A1.2.20	Disaster recovery plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.	Inspected the disaster recovery plans for the corporate headquarters and each of the in-scope colocation facilities to determine that disaster recovery plans were in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.	No exceptions noted.
A1.3: Recovery plan procedures supporting system recovery are tested to help meet the entity's availability commitments and system requirements.			
A1.3.1	IT personnel perform restoration tests of badge access control system production server backup files on at least an annual basis to help ensure recoverability.	Inquired of database administrator regarding backup restorations to determine that IT personnel performed restoration tests of badge access control system production server backup files on at least an annual basis to ensure recoverability.	No exceptions noted.
		Inspected the results of the most recent backup restoration tests for a sample of production servers supporting the badge access control system to determine that restoration tests were performed for the badge access control system production server backup files during the review period for each server sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.3.2	Disaster recovery plans are tested on at least an annual basis.	Inquired of the senior vice president (SVP) of engineering and products regarding disaster recovery testing to determine that disaster recovery plans were tested on at least an annual basis.	No exceptions noted.
		Inspected the results of the most recently completed disaster recovery tests for the corporate headquarters and each of the in-scope colocation facilities to determine that disaster recovery plans were tested during the review period.	No exceptions noted.