# SOC 1 REPORT

**FOR THE**

## COLOCATION SERVICES

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

FOR THE PERIOD JULY 1, 2014, TO JUNE 30, 2015

PREPARED IN ACCORDANCE WITH THE
AICPA SSAE NO. 16 STANDARD

Attestation and Compliance Services

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

If report recipient is not a specified user (herein referred to as a "non-specified user"), use of this report is the non-specified user's sole responsibility and at the non-specified user's sole and exclusive risk. Non-specified users may not rely on this report and do not acquire any rights against BrightLine CPAs & Associates, Inc. as a result of such access. Further, BrightLine CPAs & Associates, Inc. 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:

We have examined CoreSite Realty Corporation's ("CoreSite" or the "service organization") description of its information technology general control system for the colocation services at the data center facilities listed in Section 3 of this report throughout the period July 1, 2014, to June 30, 2015, (the "description") and the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description. The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls contemplated in the design of CoreSite's controls are suitably designed and operating effectively, along with related controls at the service organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

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

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period July 1, 2014, to June 30, 2015.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of the service organization's controls to achieve the related control objectives stated in the description involves performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of those controls to achieve the related control objectives stated in the description. 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 achieve the related control objectives stated in the description. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related control objectives stated in the description were achieved. An examination engagement of this type also includes evaluating the overall presentation of the description and the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization and described in Section 2. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Because of their nature, controls at a service organization may not prevent, or detect and correct, all errors or omissions in its information technology general control system. 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 achieve the related control objectives is subject to the risk that controls at a service organization may become inadequate or fail.

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

a. the description fairly presents the information technology general control system for the colocation services that was designed and implemented throughout the period July 1, 2014, to June 30, 2015;

b. the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively

throughout the period July 1, 2014, to June 30, 2015, and user entities applied the complementary user entity controls contemplated in the design of CoreSite's controls throughout the period July 1, 2014, to June 30, 2015; and

c. the controls tested, which together with the complementary user entity controls referred to in the scope paragraph of this report, if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period July 1, 2014, to June 30, 2015.

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

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

This report, including the description of the tests of controls and results thereof in the Testing Matrices, is intended solely for the information and use of CoreSite, user entities of CoreSite's information technology general control system for the colocation services during some or all of the period July 1, 2014, to June 30, 2015, and the independent auditors of such user entities, who have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

BrightLine CPAs & Associates, Inc.

Tampa, Florida
July 30, 2015

# SECTION 2

## MANAGEMENT'S ASSERTION

# MANAGEMENT'S ASSERTION

We have prepared the description of CoreSite Realty Corporation's ("CoreSite" or the "service organization") information technology general control system for the colocation services for user entities of the system during some or all of the period July 1, 2014, to June 30, 2015, (the "description"), and their user auditors who have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements.

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

a. the description fairly presents CoreSite's information technology general control system made available to user entities of the system during some or all of the period July 1, 2014, to June 30, 2015. The criteria we used in making this assertion were that the description

   i. presents how the system made available to user entities was designed and implemented, including:

      (1) the types of services provided;

      (2) the procedures, within both automated and manual systems, by which requests for services are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports presented to user entities of the system;

      (3) how the system captures and addresses significant events and conditions;

      (4) the process used to prepare reports or other information provided for user entities of the system;

      (5) specified control objectives and controls designed to achieve those objectives, including as applicable, complementary user entity controls contemplated in the design of our controls; and

      (6) other aspects of our control environment, risk assessment process, information and communication systems, control activities, and monitoring controls that are relevant to the services provided to user entities of the system.

   ii. does not omit or distort information relevant to the scope of CoreSite's information technology general control system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and their user auditors, and may not, therefore, include every aspect of the colocation services information technology general control system that each individual user entity of the system and its user auditor may consider important in its own particular environment; and

   iii. includes relevant details of changes to the information technology general control system for the colocation services during the period July 1, 2014, to June 30, 2015.

b. the controls related to the control objectives stated in the description were suitably designed and operated effectively throughout the period July 1, 2014, to June 30, 2015, to achieve those control objectives. The criteria we used in making this assertion were that

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

   ii. the controls identified in the description would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved and user entities applied the complementary user entity controls contemplated in the design of our controls; and

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

# SECTION 3

## DESCRIPTION OF THE SYSTEM

# Overview of Operations

### Company Background

CoreSite is engaged in the business of owning, acquiring, constructing, and managing technology-related real estate, and as of June 30, 2015, CoreSite's property portfolio included 17 operating data center facilities.

The company has built and managed data centers across the United States since 2001, offering approximately 2.7 million net rentable square feet of data center space and colocation services to more than 800 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, the following:

- Physical security and access monitoring capabilities
- Climate controls and cooling systems
- Fire detection and suppression systems
- 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** | 273,100+ square feet<br>Access to over 50 network and cloud service providers<br>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<br>Rooftop space available |
| **Fit Out** | Powered shell, infrastructured shell, and turn-key |
| **Power** | AC and DC |
| **Redundancy** | 2N, N+1 uninterruptible power supply (UPS) systems<br>N+1 generators |
| **Certifications** | Energy Star |
| **Security** | Key card access<br>Biometric scanners<br>Mantrap entry<br>Perimeter and interior IP-DVR cameras<br>24x7x365 security by CoreSite security officers<br>Controlled site access |

## MI1

CoreSite's MI1 data center in Miami provides connectivity from the U.S. to South America, as well as existing and scalable connectivity to 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, CDNs, cloud computing and IT service providers.

| | |
|---|---|
| **Features / Size** | 43,330 square feet of colocation space |
| | Access to more than 30 natively deployed network and cloud providers, as well as tethered network communications hubs nearby |
| | Access to CoreSite's Any2 Exchange® for Internet peering and Blended IP |
| **Deployments** | Cabinets, cages, private suites, and build-to- suit |
| | Rooftop space available |
| **Fit Out** | Powered shell, infrastructured shell, and turn-key |
| **Power** | AC and DC |
| **Redundancy** | 2N UPS |
| | N+1 generator |
| **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, NJ, customers benefit from scalable data center deployments within the market.

| | |
|---|---|
| **Features / Size** | 48,000+ square feet of colocation 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, NYIIX and DE-CIX |
| **Deployments** | Cabinets and cages |
| | Rooftop space available |
| **Fit Out** | Turn-key |
| **Power** | AC and DC |
| **Redundancy** | N and 2N UPS systems |
| | N+1 generator |
| **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** | 247,000+ square feet of colocation space Built above the 500-year flood plain<br>Access to the CoreSite Open Cloud Exchange and Any2 Exchange® for Internet peering, as well as leading cloud providers such as AWS Direct Connect<br>Access to leading peering exchanges, such as NYIIX and DE-CIX |
| **Deployments** | Cabinets, cages, private suites, and build-to-suit<br>Rooftop space available |
| **Fit Out** | Powered shell, infrastructured shell, and turn-key |
| **Power** | AC and DC |
| **Redundancy** | N, N + 1 and 2N UPS systems and generators |
| **Certifications** | Energy Star<br>LEED |
| **Security** | Key card access<br>Biometric scanners<br>Mantrap entries<br>Perimeter and interior IP-DVR cameras<br>24x7x365 security by CoreSite security officers<br>8' perimeter fence with controlled site access |

## Reston Campus (VA1 and VA2)

CoreSite's Reston data center campus includes two facilities, VA1 and VA2, totaling over 390,000 square feet of colocation space. Designed to create a scalable and reliable option for enterprises, networks, and cloud providers looking to expand operations and reduce costs, CoreSite's Reston campus provides direct, low-latency access to and from Ashburn and Washington, D.C.

| | |
|---|---|
| **Features / Size** | 390,000+ square feet of colocation space Metro connectivity to DC1 in Washington, D.C.<br>Access to the CoreSite Open Cloud Exchange and Any2 Exchange® for Internet peering, as well as leading cloud providers such as AWS Direct Connect |
| **Deployments** | Cabinets, cages, and private suites<br>Rooftop space available |
| **Fit Out** | Turn-key |
| **Power** | AC and DC |
| **Redundancy** | 2N, N+1 UPS systems<br>N+1 generator |
| **Security** | Key card access<br>Biometric scanners<br>Double mantrap entries<br>Perimeter and interior IP-DVR cameras<br>24x7x365 security by CoreSite security officers<br>Controlled site access |

## DC1

CoreSite's DC1 data center is located 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, VA campus.

| | |
|---|---|
| **Features / Size** | 22,000+ square feet of colocation space<br>Diverse dark fiber and DWDM connectivity to CoreSite's Reston, VA campus<br>Access to the CoreSite Open Cloud Exchange and Any2 Exchange® for Internet peering, as well as leading cloud providers such as AWS Direct Connect |
| **Deployments** | Cabinets and cages<br>Rooftop space available |
| **Fit Out** | Turn-key |
| **Power** | AC and DC |
| **Redundancy** | 2N UPS systems<br>Single generator |
| **Security** | Key card access<br>Biometric scanners<br>Camera-monitored entries<br>Perimeter and interior IP-DVR cameras<br>Controlled site access |

## CH1

CoreSite's CH1 facility is strategically located in downtown Chicago, adjacent to the Board of Trade. This centralized location provides access to exceptionally low-latency connections for the many financial, healthcare and media companies deployed within CH1.

| | |
|---|---|
| **Features / Size** | 178,000+ square feet of colocation space<br>Access to over 50 network and cloud service providers<br>Access to the CoreSite Open Cloud Exchange and Any2Exchange® for Internet Peering |
| **Deployments** | Cabinets, cages, and private suites<br>Rooftop space available |
| **Fit Out** | Turn-key |
| **Power** | AC and DC |
| **Redundancy** | N, N+1, 2N UPS systems<br>N+1 generator |
| **Security** | Key card access<br>Biometric scanners<br>Mantrap entries<br>Perimeter and interior IP-DVR cameras<br>24x7x365 security guard monitoring<br>Controlled site access |

## SV1

CoreSite's SV1 facility serves as the carrier hub for CoreSite's tethered Silicon Valley data center campus. More than 90 customers, including international and national carriers, social media companies, cloud computing providers, media and entertainment firms and enterprises make up the high-performance ecosystem of SV1.

| | |
|---|---|
| **Features / Size** | 84,000+ square feet of colocation space |
| | Critical data center gateway for sub-sea cables to the Asia Pacific market |
| | Access to the CoreSite Open Cloud Exchange and Any2 Exchange® for Internet peering, as well as leading cloud providers such as AWS Direct Connect |
| **Deployments** | Cabinets, cages, and private suites |
| | Rooftop space available |
| **Fit Out** | Turn-key |
| **Power** | AC and DC |
| **Redundancy** | 2N or N+1UPS systems |
| | Single generator |
| **Security** | Key card access |
| | 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 |
| | Centrally located in the heart of the world's most influential technology companies |
| | Access to the CoreSite Open Cloud Exchange and Any2 Exchange® for Internet peering, as well as leading cloud providers such as AWS Direct Connect |
| **Deployments** | Cabinets, cages, and private suites |
| | Rooftop space available |
| **Fit Out** | Turn-key |
| **Power** | AC and DC |
| **Redundancy** | N, N+1, 2N UPS systems |
| | N and 2N generators |
| **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, Any2Exchange® for Internet peering, and more than 100 networks, on-net carriers, and ISPs.

| | |
|---|---|
| **Features / Size** | 50,000 square feet |
| **Deployments** | Cages and private suites |
| **Fit Out** | Turn-key |
| **Power** | AC and DC |
| **Redundancy** | 2N UPS systems<br>N+1 generator |
| **Security** | Key card access<br>Security guard station at the facility main entrance<br>Biometric scanners<br>Perimeter and interior IP-DVR cameras<br>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 our 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 colocation space<br>Raised floor colocation space to meet the needs of the highest-density customer requirements<br>Access to the CoreSite Open Cloud Exchange and Any2 Exchange® for Internet peering, as well as leading cloud providers such as AWS Direct Connect |
| **Deployments** | Cabinets, cages, private suites, and build-to-suit<br>Rooftop space available |
| **Fit Out** | Turn-key |
| **Power** | AC and DC |
| **Redundancy** | 2N or N+1 UPS systems<br>N+1 generator |
| **Security** | Key card access<br>Biometric scanners<br>Mantrap entries<br>Perimeter and interior IP-DVR cameras<br>24x7x365 security guard monitoring<br>8' perimeter fence with controlled site access |

## LA1

CoreSite's LA1 facility, also known as One Wilshire®, is one of the most densely interconnected data centers in the world. Home to nearly 200 networks and nearly 60 cloud and IT service providers, LA1 provides access to a multitude of interconnections and service partners for its customer ecosystem

| | |
|---|---|
| **Features** | 139,000+ square feet of colocation space<br>Tethered to CoreSite's LA2 data center via high-count dark-fiber<br>Native access to the CoreSite Open Cloud Exchange and Any2 Exchange® for Internet peering, as well as leading cloud providers such as AWS Direct Connect<br>Industry-leading connectivity to Asia-Pacific markets |
| **Deployments** | Cabinets, cages, and private suites<br>Rooftop space available |
| **Fit Out** | Turn-key |
| **Power** | AC and DC |
| **Redundancy** | N, N+1, 2N UPSs, PDUs, and RPPs<br>N+1 generator |
| **Security** | Key card access<br>Biometric scanners<br>Double mantrap entry<br>Perimeter and interior IP-DVR cameras<br>Controlled site access |

## LA2

CoreSite's LA2 facility provides data center scalability within the Los Angeles market. Over 200 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 colocation space<br>Tethered to CoreSite's LA campus via high-count dark-fiber<br>Access to the CoreSite Open Cloud Exchange and Any2 Exchange® for Internet peering, as well as leading cloud providers such as AWS Direct Connect |
| **Deployments** | Cabinets, cages, private suites, and build-to-suit<br>Rooftop space available |
| **Fit Out** | Powered shell, infrastructured shell, and turn-key |
| **Power** | AC and DC |
| **Redundancy** | N, N+1, 2N UPS systems<br>N+1 generator |
| **Security** | Key card access<br>Biometric scanners<br>Double mantrap entry<br>Perimeter and interior IP-DVR cameras<br>24x7x365 security guard monitoring<br>Controlled site access |

## DE1

Located in the center of downtown Denver at the nexus of fiber plants of multiple national and regional carriers and network service providers, DE1 facilitates a rich interconnection environment. In addition to the 30+ carriers, DE1 hosts multiple cloud providers and operates the Any2Exchange® (formerly the Rocky Mountain Internet Exchange), which is the largest peering exchange in the region.

| | |
|---|---|
| **Features / Size** | 5,800+ square feet<br>Hub of communications for the Rocky Mountain region<br>100% uptime service level agreement (SLA)<br>Any2Exchange® for internet peering<br>Nearly limitless connectivity options<br>Blended IP service |
| **Deployments** | Full, half, and quarter cabinets |
| **Fit Out** | Turn-key |
| **Power** | AC and DC |
| **Redundancy** | N, 2N UPS systems<br>Single generator |
| **Security** | Key card access<br>Interior IP cameras<br>Controlled site access<br>Biometric scanners |

## DE2

Sitting adjacent to Level 3's gateway and with direct access to CoreSite's DE1 facility, DE2 provides simple access to all major carriers servicing the Rocky Mountain Region. Further, customers can access the Any2Exchange® for Internet peering (formerly the Rocky Mountain Internet Exchange), which is the largest exchange in the region.

| | |
|---|---|
| **Features / Size** | 5,100+ square feet<br>100% uptime SLA<br>Any2Exchange® for internet peering<br>Blended IP service |
| **Deployments** | Full, half, and quarter cabinets<br>Rooftop space available |
| **Fit Out** | Turn-key |
| **Power** | AC and DC |
| **Redundancy** | N, N+1 UPS systems<br>Single generator |
| **Security** | Key card access<br>Interior IP cameras<br>Controlled site access<br>Biometric scanners |

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 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 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 SONET/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 Dense Wave Division Multiplexers (DWDM) line cards on a single DWDM chassis.

*Any2 Peering Exchange*

Any2 is a layer 2, IPv6-supporting, physical network switch operated by CoreSite to facilitate the exchange of Internet traffic between 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 ARIN or 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 POP within a CoreSite data center) and is open to further federation with other non-profit or regional exchanges.

**Boundaries of the System**

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

Customer requests for services are initiated and authorized by user entities as described within the Technical Support to Customers control objective.

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

| Metro Area | Name | Address |
|---|---|---|
| Boston, Massachusetts | BO1 | 70 Innerbelt |
| Miami, Florida | MI1 | 2115 NW 22nd Street |
| New York, New York | NY1 | 32 Avenue of the Americas |
| Secaucus, New Jersey | NY2 | 2 Emerson Lane |
| Reston, Virginia | VA1 | 12100 Sunrise Valley |

| Metro Area | Name | Address |
|---|---|---|
| Reston, Virginia | VA2 | 12100 Sunrise Valley |
| Washington, DC | DC1 | 1275 K Street |
| Chicago, Illinois | CH1 | 427 S LaSalle |
| San Jose, California | SV1 | 55 S Market |
| Milpitas, California | SV2 | 1656 McCarthy |
| Santa Clara, California | SV3 | 2901 Coronado |
| Santa Clara, California | SV4 | 2972 Stender Way |
| Los Angeles, California | LA1 | One Wilshire |
| Los Angeles, California | LA2 | 900 N Alameda |
| Denver, Colorado | DE1 | 910 15th Street |
| Denver, Colorado | DE2 | 639 E 18th Avenue |

*Subservice Organizations*

No subservice organizations were included in the scope of this assessment.

*Significant Changes during the Review Period*

The VA2 data center located at 12100 Sunrise Valley, Reston, Virginia, was placed into service in April 2015. The reliability of power, reliability of data center cooling, security of premises, and technical support to customers were excluded from the scope of this report for the period of July 2014, through April 2015 (the period prior to the service go-live date for VA2).

*Functional Areas of Operations*

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
- Facilities and operations management – responsible for overseeing day-to-day operations of the data center facilities and responding to customer inquiries

*Infrastructure*

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 fingerprint 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 (AD). Authorized users have the ability to remotely access the production network via transport layer security (TLS) encrypted virtual private network (VPN) connections. 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 the in-house developed Operations Support System (OSS) ticketing system utilized 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 OSS ticketing system 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 OSS 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:

| 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 fingerprint 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 |
| Firewall System | Utilized to filter and route traffic to and from the production network | Check Point | Reston, Virginia; Los Angeles, California; Denver, Colorado |
| VPN | Utilized for remote access to the production network | Windows Virtual Machine | Denver, Colorado |

*Data Management*

The colocation services system provided by CoreSite does not provide any services directly related to the initiation, authorization, and processing of transactions. The colocation services provided by CoreSite allow for the availability of the systems user entities utilize to perform the procedures, both automated and manual, related to the initiation, authorization and processing of transactions.

# 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; the oversight and direction provided by the board of directors and audit committee; its organizational structure; management's commitment to competence; and accountability through management's philosophy and operating style and human resources (HR) policies and practices.

### 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 practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, 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.
- HR personnel perform background checks for employment candidates as a component of the hiring process.
- Employees are required to complete ethics training within 30 days of hiring and all employees take ethics training on an annual basis.

### 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 key areas of authority, responsibility and lines of reporting.

### Commitment to Competence

CoreSite's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. 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 senior 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.
- 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 control objectives 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 significance of identified risks, assessing the likelihood of their occurrence, and determining actions to address them. However, because control objectives relate to risk(s) that controls seek to mitigate, management thoughtfully identified control objectives when designing, implementing, and documenting their system.

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. CoreSite has established risk factor categories, including:

- Financial
- Operational
- Accounting and disclosure
- Information
- Ethical
- Human capital
- Information technology
- External

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

### Integration with Control Objectives

Along with assessing risks, management has identified and put into effect actions needed to address those risks. In order to address risks, control 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 those objectives.

## CONTROL OBJECTIVES AND RELATED CONTROL ACTIVITIES

### Selection and Development of Control Activities

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

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

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

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

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

### Reliability of Power

Control Objective: Control activities provide reasonable assurance that the design, maintenance, and operation of power infrastructure are sufficient to power colocation space.

CoreSite has controls in place to support the reliability of 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 through the use of 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 on a monthly basis 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. 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.

**Reliability of Data Center Cooling**

Control Objective: Control activities provide reasonable assurance that the design, maintenance, and operation of cooling infrastructure are sufficient to cool colocation space.

CoreSite has controls in place to support the reliability of data center cooling for its colocation facilities. CoreSite utilizes multiple air 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 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.

**Security of Premises**

Control Objective: Control activities provide reasonable assurance that the design, maintenance, and operations of security systems are sufficient to secure the premises.

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 third party or internal 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. The badge access control systems are configured to log ingress and egress activity at colocation facilities, maintaining a history available for review as needed. Employee badge access privileges are granted based on individual job responsibilities and revoked as a component of the employee transfer or termination processes. 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, and are issued a temporary badge for use while within the colocation facilities. 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 operations support 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 as needed. Lastly, alarm panels are in place within the colocation facilities and security guards are alerted when an alarm panel is triggered.

**Technical Support to Customers**

Control Objective: Control activities provide reasonable assurance that the system for customer cabinet and cage installations, provisioning or interconnections, and trouble-ticket response is adhered to in accordance with guidelines.

CoreSite maintains documented policies and procedures to guide personnel in providing technical support services to customers. The procedures address customer installations, ongoing support, and troubleshooting.

CoreSite maintains an operations support system to track, manage, and resolve issues related to the services provided to customers. The operations support system has an online customer portal that customers utilize to enter trouble tickets, work orders, and remote hands tickets. The operations support system is configured to e-mail a copy of the trouble ticket to the originator of the trouble ticket, work order, or remote hands ticket. Tickets directly entered through the operations support system trigger an e-mail containing details of the ticket to the operations group. Upon receipt of tickets, members of the operations group acknowledge receipt and work the tickets to completion. Requests for cabinet and cage installations and interconnection requests are also entered and tracked in the operations support system. Issues regarding cabinet and cage installation requests, interconnection requests, and trouble tickets are reviewed at an operations meeting on a bi-weekly basis. Additionally closed cabinet and cage installation requests, interconnection requests, and trouble tickets are retained in the operations support system for historical review and tracking purposes.

To help ensure technical support can be provided to customers as needed, on-site operations support is available during extended business hours and on-call operations support is available 24 hours per day at colocation facilities.

## 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 onsite 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 OSS ticketing system 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 is able to 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 Activities

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. Internal audit records and tracks identified deficiencies.

Additionally, 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 SSAE 16 (SOC 1) examinations

- 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 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.

**Reporting 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

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

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

*Reliability of Data Center Power*

1. User entities are responsible for defining power requirements and notifying CoreSite of any changes to the power requirements.

*Security of Premises*

2. User entities are responsible for determining whether CoreSite's security infrastructure is appropriate for its needs and for notifying the service organization of any requested modifications.
3. User entities are responsible for reading and adhering to CoreSite's policies and procedures regarding conduct in the data center.
4. User entities are responsible for maintaining their own asset control processes and policies and for insuring their equipment housed within the CoreSite data centers.
5. User entities are responsible for notifying CoreSite of on-site visits of employees, vendors, and contractors prior to their arrival to the data center.

6. User entities are responsible for informing their vendors of the CoreSite's policies and procedures regarding conduct in the data center.
7. User entities are responsible for ensuring their guests/visitors are escorted, as appropriate, throughout CoreSite's data centers.
8. User entities are responsible for providing CoreSite the listing of individuals authorized to access the data center and customer cage and for notifying CoreSite if an individual should be removed from the access list.
9. User entities are responsible for ensuring their cabinets or racks are locked and their equipment is secured prior to leaving the premises.

*Technical Support to Customers*

10. User entities are responsible for notifying CoreSite of changes made to technical or administrative contact information.
11. User entities are responsible for designating authorized individuals to issue work requests.

# 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 considered to be relevant to the internal control over financial reporting of respective user entities. BrightLine conducted the examination testing over the period July 1, 2014, through June 30, 2015.

### Tests of Operating Effectiveness

The tests applied to test the operating effectiveness of controls are listed alongside each of the respective control activities within the Testing Matrices. Such tests were considered necessary to evaluate whether the controls were sufficient to provide reasonable, but not absolute, assurance that the specified control objectives were achieved during the review period. In selecting the tests of controls, BrightLine 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;
- 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 authoritative literature, BrightLine 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. BrightLine selected samples in such a way that the samples were expected to be representative of the population. This included judgmental selection methods, where applicable, to ensure representative samples were obtained.

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

**Test Results**

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

## RELIABILITY OF POWER

**Control Objective Specified by the Service Organization:** Control activities provide reasonable assurance that the design, maintenance, and operation of power infrastructure are sufficient to power colocation space.

| # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| 1.01 | The power infrastructure for the colocation facilities is configured to provide redundancy for power systems. | 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 for the colocation facilities during the review period 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. |
| 1.02 | 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. |

| # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | | Observed the presence of multiple UPS systems during the review period to determine that multiple UPS systems were in place at the colocation facilities. | No exceptions noted. |
| 1.03 | 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 help ensure proper functioning. | No exceptions noted. |
| | | Inspected the third party vendor service agreements and the most recent preventative maintenance results or invoices to determine that third party vendors inspected and maintained the UPS systems during the review period. | No exceptions noted. |
| 1.04 | 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 help 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 for each month sampled. | No exceptions noted. |
| 1.05 | 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 help ensure proper functioning. | No exceptions noted. |
| | | Inspected the third party vendor service agreements and inspection reports or invoices 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. |

| # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| 1.06 | Power supply equipment owned and managed by CoreSite is monitored by building automation systems. | Inspected the building automation systems to determine that power supply equipment was monitored by building automation systems | No exceptions noted. |
| 1.07 | The building automation systems are configured to alert operations personnel when predefined alarms are triggered. | 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 alarms were triggered. | No exceptions noted. |

## RELIABILITY OF DATA CENTER COOLING

**Control Objective Specified by the Service Organization:** Control activities provide reasonable assurance that the design, maintenance and operation of cooling infrastructure are sufficient to cool colocation space.

| # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| 2.01 | Multiple air handlers are in place to cool the colocation facilities and provide redundancy. | Inquired of data center and operations personnel regarding air handlers to determine that multiple air handlers were in place to cool the colocation facilities and provide redundancy. | No exceptions noted. |
| | | Observed the presence of multiple air handlers and chiller tanks, as applicable, during the review period to determine that multiple air handlers and water chillers were in place at the colocation facilities. | No exceptions noted. |
| 2.02 | 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 help ensure proper functioning. | No exceptions noted. |

| # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | | Inspected the third party vendor service agreements and the preventive maintenance results or invoices 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. |
| 2.03 | 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 to determine that the building automation systems were configured to monitor environmental conditions, including temperature and humidity levels, at the colocation facilities. | No exceptions noted. |
| 2.04 | The building automation systems are configured to alert operations personnel when predefined thresholds are exceeded 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 on monitored systems. | No exceptions noted. |
| 2.05 | The colocation facilities are equipped with fire detection and suppression controls that include the following:<br>• Audible and visual fire alarms<br>• Dry-pipe water sprinklers or FM-200 fire suppression systems<br>• Fire and smoke detectors<br>• 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:<br>• Audible and visual fire alarms<br>• Dry-pipe water sprinklers or FM-200 fire suppression systems<br>• Fire and smoke detectors<br>• Hand-held fire extinguishers | No exceptions noted. |

| # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| 2.06 | 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 inspection reports or invoices to determine that third party vendors inspected the fire detection and suppression equipment during the review period. | The test of the control activity disclosed the following:<br>• The dry-pipe sprinkler system at the SV3 data center facility was last inspected in February 2014.<br>• The audible and visual fire alarms, dry-pipe sprinkler system and fire and smoke detectors at the SV4 data center facility were last inspected in March 2014.<br><br>No exceptions were noted for the BO1, MI1, NY1, NY2, VA1, VA2, DC1, CH1, SV1, SV2, LA1, LA2, DE1, or DE2 data center facilities. |

## SECURITY OF PREMISES

**Control Objective Specified by the Service Organization:** Control activities provide reasonable assurance that the design, maintenance and operations of security systems are sufficient to secure the premises.

| # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| 3.01 | A security procedures manual is in place to guide personnel in carrying out the following security procedures and related activities:<br>• Access control system<br>• Visitor management<br>• Deliveries<br>• Property removal<br>• 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:<br>• Access control system<br>• Visitor management<br>• Deliveries<br>• Property removal<br>• Support services | No exceptions noted. |
| 3.02 | 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 personnel regarding security monitoring to determine that physical security at the DE2 colocation facility was monitored remotely. | No exceptions noted. |

| # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | | Observed the security guards at the facilities during the review period to determine that security guards monitored physical security at the applicable colocation facilities. | No exceptions noted. |
| | | Inspected the security guard staffing schedule to determine that on-site third party or internal security guards monitored physical security at the applicable colocation facilities. | No exceptions noted. |
| 3.03 | Badge access control systems are in place to control access to and within the colocation facilities. | Observed the badge access control systems in place throughout the colocation facilities during the review period 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 to determine that badge access control systems were in place to control access to and within the colocation facilities. | No exceptions noted. |
| 3.04 | The ability to administer the badge access control system is restricted to user accounts accessible by authorized personnel. | Inquired of data center and operations personnel regarding the ability to administer the badge access control system to determine that the ability to administer the badge access system was restricted to user accounts accessible by authorized personnel. | No exceptions noted. |
| | | Inspected the listing of users with administrative access rights to the badge access control system to determine that the ability to administer the badge access system was restricted to user accounts accessible by authorized personnel. | No exceptions noted. |

| # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| 3.05 | The badge access control system is configured to log egress and ingress activity. | Inspected example badge access control system logs generated during the review period to determine that the badge access control system was configured to log egress and ingress activity. | No exceptions noted. |
| 3.06 | Badge access privileges are revoked as a component of the employee termination process. | Inquired of data center and operations personnel regarding badge access revocation to determine that badge access privileges were revoked as a component of the employee termination process. | No exceptions noted. |
| | | Inspected the badge access control system user listings for a sample of employees terminated during the review period to determine that badge access privileges were revoked for each terminated employee sampled. | No exceptions noted. |
| 3.07 | Visitors are required to provide photo identification, to be logged in the badge access control systems, and are issued a temporary badge for use while within the colocation facilities. | Observed the visitor entrance procedures during the review period to determine that visitors were required to provide photo identification to be logged in the badge access control systems and were issued a temporary badge for use while within the colocation facilities. | The test of the control activity disclosed that visitors were not required to provide photo identification, were not logged in the badge access control system, and were not issued a temporary badge for the DE1 or DE2 data center facilities; however, visitors to the DE1 and DE2 data center facilities were escorted while onsite.<br><br>No exceptions were noted for the BO1, MI1, NY1, NY2, VA1, VA2, DC1, CH1, SV1, SV2, SV3, SV4, LA1, or LA2 data center facilities. |
| | | Inspected the visitor logs from the badge access control systems for a sample of dates during the review period to determine that visitors were logged in the badge access control systems for each date sampled. | The test of the control activity disclosed that visitor logs were not in place for the DE1 or DE2 data center facilities.<br><br>No exceptions were noted for the BO1, MI1, NY1, NY2, VA1, VA2, DC1, CH1, SV1, SV2, SV3, SV4, LA1, or LA2 data center facilities. |

| # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| 3.08 | Physical key inventory listings are maintained, as applicable, to track physical key assignments. | Inquired of data center and operations personnel regarding the physical key inventory listings to determine that physical key inventory listings were maintained, as applicable, to track physical key assignments. | No exceptions noted. |
| | | Inspected the physical key inventory listings to determine that physical key inventory listings were maintained, as applicable, to track physical key assignments. | No exceptions noted. |
| 3.09 | An operations support system is utilized to process and track requests that include the following:<br>• Service appointments<br>• Deliveries<br>• Property removal<br>• Construction<br>• Access requests, modifications and deletions | Inspected the operations support system and an example ticket processed during the review period to determine that an automated operations support system was utilized to process and track the following requests:<br>• Service appointments<br>• Deliveries<br>• Property removal<br>• Construction<br>• Access requests, modifications and deletions | No exceptions noted. |
| 3.10 | Deliveries are required to be logged into the operations support system. | Inspected the package delivery log and a sample of tickets processed during the review period to determine that deliveries were required to be authorized and logged. | No exceptions noted. |
| 3.11 | Network video recorder (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 throughout the colocation facilities during the review period to determine that NVR camera systems were in place. | No exceptions noted. |

| # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| 3.12 | 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 a sample of historical NVR images archived during the review period to determine that NVR images were retained for a minimum of 90 days. | No exceptions noted. |
| 3.13 | 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 within the colocation facilities during the review period to determine that security guards were alerted when an alarm panel was triggered. | No exceptions noted. |

## TECHNICAL SUPPORT TO CUSTOMERS

**Control Objective Specified by the Service Organization:** Control activities provide reasonable assurance that the system for customer cabinet and cage installations, provisioning or interconnections, and trouble-ticket response is adhered to in accordance with guidelines.

| # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| 4.01 | Documented procedures are in place to guide personnel in customer installations and troubleshooting. | Inspected the security procedures manual to determine that procedures were documented to guide personnel in customer installations and troubleshooting. | No exceptions noted. |
| | **Operations Group Availability** | | |
| 4.02 | On-call operations support is available 24 hours per day. | Inquired of data center and operations personnel regarding on-call support to determine that on-call operations support was available 24 hours per day. | No exceptions noted. |

| # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | | Inspected a sample of operations shift schedules to determine that on-call operations support was available 24 hours per day. | No exceptions noted. |
| 4.03 | Operations support is available on-site during extended business hours. | Inquired of data center and operations personnel regarding on-site support to determine that operations support was available on-site during extended business hours. | No exceptions noted. |
| | | Inspected the operations shift schedules and escalation procedures to determine that operations support was available on-site during extended business hours. | No exceptions noted. |
| | **Trouble Ticket Response** | | |
| 4.04 | Customers enter trouble tickets through the customer portal of the operations support system. | Inquired of data center and operations personnel regarding the operations support system to determine that customers entered trouble tickets through the customer portal of the operations support system. | No exceptions noted. |
| | | Inspected a sample of operations support system tickets processed during the review period to determine that customers entered trouble tickets through the customer portal of the operations support system. | No exceptions noted. |
| 4.05 | Trouble tickets directly entered through the operations support system trigger an e-mail containing details of the trouble ticket to the operations group. | Inspected the operations support system notification configurations and the e-mail notification for an example ticket generated during the review period to determine that trouble tickets directly entered through the operations support system triggered an e-mail containing details of the trouble ticket to the operations group. | No exceptions noted. |
| 4.06 | The operations support system is configured to e-mail a copy of the trouble ticket to the originator of the trouble ticket. | Inquired of data center and operations personnel regarding the operations support system to determine that the operations support system was configured to e-mail a copy of the trouble ticket to the originator of the ticket. | No exceptions noted. |

| # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | | Inspected the e-mail notification for an example ticket generated during the review period to determine that the operations support system was configured to e-mail a copy of the trouble ticket to the originator of the ticket. | No exceptions noted. |
| | **Cabinet and Cage Installation Requests** | | |
| 4.07 | Cabinet and cage installation requests are entered and tracked in the operations support system. | Inquired of data center and operations personnel regarding the operations support system to determine that cabinet and cage installation requests were entered and tracked in the operations support system. | No exceptions noted. |
| | | Inspected a sample of tickets processed during the review period to determine that cabinet and cage installation requests were entered and tracked in the operations support system. | No exceptions noted. |
| | **Provision of Interconnections** | | |
| 4.08 | Interconnection requests are entered and tracked in the operations support system. | Inquired of data center and operations personnel regarding the operations support system to determine that interconnection requests were entered and tracked in the operations support system. | No exceptions noted. |
| | | Inspected a sample of tickets processed during the review period to determine that interconnection requests were entered and tracked in the operations support system. | No exceptions noted. |
| | **Cabinet and Cage Installation Requests, Interconnection Requests and Trouble Ticket Monitoring** | | |
| 4.09 | 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. |

| # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | | Inspected the recurring calendar invitation and listing of invitees for the operations meetings to determine that operations meetings were held on a weekly basis. | No exceptions noted. |
| 4.10 | Closed cabinet and cage installation requests, interconnection requests and trouble tickets are retained in the operations support system. | Inquired of data center and operations personnel regarding the operations support system to determine that closed cabinet and cage installation requests, interconnection requests and trouble tickets were retained in the operations support system. | No exceptions noted. |
| | | Inspected the operations support system configurations to determine that closed cabinet and cage installation requests, interconnection requests and trouble tickets were retained in the operations support system. | No exceptions noted. |

# SECTION 5

## OTHER INFORMATION PROVIDED BY MANAGEMENT

# MANAGEMENT'S RESPONSE TO TESTING EXCEPTIONS

**Reliability of Data Center Cooling**

| # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| 2.06 | 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 inspection reports or invoices to determine that third party vendors inspected the fire detection and suppression equipment during the review period. | The test of the control activity disclosed the following:<br>• The dry-pipe sprinkler system at the SV3 data center facility was last inspected in February 2014.<br>• The audible and visual fire alarms, dry-pipe sprinkler system and fire and smoke detectors at the SV4 data center facility were last inspected in March 2014.<br><br>No exceptions were noted for the BO1, MI1, NY1, NY2, VA1, VA2, DC1, CH1, SV1, SV2, LA1, LA2, DE1, or DE2 data center facilities. |
| **Management's Response:** | Inspection of the dry-pipe sprinkler system at SV3 is scheduled for completion in August of 2015. At SV4, the fire detection and suppression equipment inspection was completed in July of 2015. CoreSite will review and reinforce the fire system inspection procedures with personnel at SV3 and SV4. | | |

**Security of Premises**

| # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| 3.07 | Visitors are required to provide photo identification, to be logged in the badge access control systems, and are issued a temporary badge for use while within the colocation facilities. | Observed the visitor entrance procedures during the review period to determine that visitors were required to provide photo identification to be logged in the badge access control systems and were issued a temporary badge for use while within the colocation facilities. | The test of the control activity disclosed that visitors were not required to provide photo identification, were not logged in the badge access control system, and were not issued a temporary badge for the DE1 and DE2 data center facilities; however, visitors to the DE1 and DE2 data center facilities were escorted while onsite.<br><br>No exceptions were noted for the BO1, MI1, NY1, NY2, VA1, VA2, DC1, CH1, SV1, SV2, SV3, SV4, LA1, or LA2 data center facilities. |

| # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | | Inspected the visitor logs from the badge access control systems for a sample of dates during the review period to determine that visitors were logged in the badge access control systems for each date sampled. | The test of the control activity disclosed that visitor logs were not in place for the DE1 and DE2 data center facilities.<br><br>No exceptions were noted for the BO1, MI1, NY1, NY2, VA1, VA2, DC1, CH1, SV1, SV2, SV3, SV4, LA1, or LA2 data center facilities. |
| **Management's Response:** | Visitor logs are now available and utilized as necessary at DE1 and DE2. In addition, the badge issuance process for visitors at DE1 and DE2 was reviewed with the employees on site and will be enforced going forward. | | |