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, 2015, TO JUNE 30, 2016
PREPARED IN ACCORDANCE WITH THE
AICPA SSAE NO. 16 AND IAASB ISAE 3402 STANDARDS

Attestation and Compliance Services

Proprietary & Confidential
Unauthorized use, reproduction or distribution of this report, in whole or in part, is strictly prohibited.
This report is intended solely for use by the management of Savvis Communications Corporation dba CenturyLink TS, its user entities (i.e., customers) that utilized the services covered by this report during the specified time period, and the independent financial statement auditors of those user entities (each referred to herein as a "specified user").

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

Unauthorized use, reproduction or distribution of this report, in whole or in part, is strictly prohibited.
# Table of Contents

**Section 1** Independent Service Auditor’s Report .............................................................. 1

**Section 2** Management’s Assertion .................... 4

**Section 3** Description of the System ............... 7

**Section 4** Testing Matrices ............................. 26

**Section 5** Other Information Provided by Management ................................................. 41
SECTION I
INDEPENDENT SERVICE AUDITOR’S REPORT
INDEPENDENT SERVICE AUDITOR’S REPORT

To Savvis Communications Corporation dba CenturyLink TS:

Scope

We have examined Savvis Communications Corporation dba CenturyLink TS’s (“CenturyLink” or the “service organization”) description of its colocation services system at the CenturyLink data center facilities listed in Section 3 throughout the period July 1, 2015, to June 30, 2016, (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 CenturyLink’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.

CenturyLink uses third party service organizations for colocation and building management services at certain locations specified in Section 3. The description in Section 3 includes only the control objectives and related controls of CenturyLink and excludes the control objectives and related controls of the third party service organizations. Our examination did not extend to controls at the third party service organizations.

Service organization’s responsibilities

In Section 2, CenturyLink 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. CenturyLink 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.

Service auditor’s responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination. We conducted our examination in accordance with SSAE 16, “Reporting on Controls at a Service Organization” issued by the American Institute of Certified Public Accountants and in accordance with ISAE 3402, “Assurance Reports on Controls at a Service Organization,” issued by the International Auditing and Assurance Standards Board. Those standards require that we comply with ethical requirements and 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, 2015, to June 30, 2016.

An examination of a description of a service organization’s system and the suitability of the design and operating effectiveness of the controls involves performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of 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 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.
Inherent limitations

Because of their nature, controls at a service organization may not prevent, or detect and correct, all errors or omissions in providing colocation services. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design 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.

Other information provided by the service organization

In Section 5, CenturyLink has provided additional information that is not a part of CenturyLink’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.

Opinion

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

a. the description fairly presents the colocation services system that was designed and implemented throughout the period July 1, 2015, to June 30, 2016;

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, 2015, to June 30, 2016, and user entities applied the complementary user entity controls contemplated in the design of CenturyLink’s controls throughout the period July 1, 2015, to June 30, 2016; 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, 2015, to June 30, 2016.

Description of tests of controls

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

Restricted use

This report, including the description of the tests of controls and results thereof in the Testing Matrices, is intended solely for the information and use of CenturyLink, user entities of CenturyLink’s colocation services system during some or all of the period July 1, 2015, to June 30, 2016, 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.

Scheffman & Company, LLC

Tampa, Florida
August 5, 2016
SECTION 2

MANAGEMENT’S ASSERTION
MANAGEMENT’S ASSERTION

We have prepared the description of Savvis Communications Corporations dba CenturyLink TS’s ("CenturyLink") colocation services system for user entities of the system during some or all of the period July 1, 2015, to June 30, 2016 (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 the colocation services system made available to user entities of the system during some or all of the period July 1, 2015, to June 30, 2016. CenturyLink uses third party service organizations for colocation and building management services at certain locations specified in Section 3. The description in Section 3 of this report includes only the controls and related control objectives of CenturyLink and excludes the control objectives and related controls of the third party service organizations. The criteria we used in making our assertion were that the description

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

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

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

(3) the related accounting records, supporting information, and specific accounts that are used to initiate, authorize, record, process, and report transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities of the system;

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

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

(6) 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

(7) other aspects of our control environment, risk assessment process, information and communication systems (including the related business processes), control activities, and monitoring controls that are relevant to processing and reporting transactions of user entities of the system.

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

iii. includes relevant details of changes to the colocation services system during the period July 1, 2015, to June 30, 2016.

b. the controls related to the control objectives stated in the description were suitably designed and operated effectively throughout the period July 1, 2015, to June 30, 2016, to achieve those control objectives and the third party service organizations applied the controls contemplated in the design of CenturyLink’s controls. The criteria we used in making this assertion were that

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

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

Savvis Communications Corporation dba CenturyLink TS, a division of CenturyLink (NASDAQ:CTL), is an outsourcing provider of managed computing and network infrastructure for information technology (IT) applications.

In July 2011, Savvis merged with CenturyLink, Inc. to become Savvis, A CenturyLink Company. Then in January of 2014 Savvis, a CenturyLink Company rebranded to become CenturyLink TS. For the purposes of this report, Savvis Communications Corporation dba CenturyLink TS will be referenced “CenturyLink” or the “service organization”.

CenturyLink infrastructure extends to 45 countries around the world and includes:

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

Description of Services Provided

CenturyLink provides facilities and infrastructure to protect customers’ systems from physical and environmental security threats. CenturyLink’s colocation solutions are built on the following core components:

- Multi-level physical security
- N+1 power infrastructure
- Access to CenturyLink’s multiprotocol label switching (MPLS)-enabled network and a global network footprint
- 24x7 global support service to customers, employees, partners and investors

The data centers provide hosting services in facilities that are specifically designed to provide hosting for mission-critical environments.

Colocation services consist of physical and environmental protection services including, but not limited to, the following:

- Physical security
- Heating ventilation and air conditioning (HVAC)
- Fire detection and suppression
- Power
- Network connectivity
- Remote hands
- Training personnel for onsite support

New Order Processing, Installations, and Change of Colocation Services

The CenturyLink sales organizations consult with customers to build an acceptable quote for desired products and services. Once a satisfactory solution with corresponding pricing has been developed, a signed order is obtained from the customers prior to initiation of an order. Upon receipt of the signed order, revenue is booked and the order is processed into the Delivery Management System. Once the order package is complete, the order is assigned to a project manager who supervises the customer setup and/or installation of services through
to the initiation of billing. Order requirements are detailed within either Intuitive Bookable Order Checklists (IBOC) or Bookable Order Checklists (BOC) process documents and differ per product purchased. Furthermore, documented procedures are in place for the service delivery process to help ensure that each customer receives the service(s) requested.

The project manager works with various groups/departments within CenturyLink and/or various vendors to deliver the requested services and is responsible for the successful implementation of the services requested on the customer order. Services and products listed in the signed order are documented as complete in the Delivery Management System as they are installed. The project manager, the customer, and internal departments work together to forecast an estimated order completion date, which is monitored through regular status updates. If any changes to the estimated order completion date occur, they will be communicated to the customer during status updates or through e-mail communications.

For installation of colocation services, within three business days, the customer indicates acceptance of installed services to the project manager and billing is initiated. Lack of response within three days is considered acceptance of the service.

Support for Colocation Services

CenturyLink’s Global Client Services organization operates five CenturyLink Operations Centers (OCs). The OCs are located in St. Louis, Missouri, US; Wokingham, Berkshire, England; Tokyo, Japan; Bangalore, India; and Singapore. Each OC has a mirrored functional structure to facilitate proactive customer event monitoring and manage customer-specific service requests: change management, remote support, and incident resolution.

OC representatives follow defined procedures to facilitate priority identification, customer communication of unexpected events that may impact their systems, customer authorization – only authorized customer representatives can open a service request, and functional escalation for customer service requests and incidents. Issues are documented in a ticketing system and tracked to resolution.

CenturyLink uses an event management system that is integrated with the CenturyLink Operational Support System (OSS). CenturyLink monitors events through an automated monitoring tool. Events are routed through Internet control message protocol (ICMP) (ping) pollers, Interface Monitors, or the CenturyLink Intelligent Agent (installed locally on managed servers).

The ticketing system/customer relationship management (CRM) system contains a complete purchased product hierarchy, installed equipment, and the physical and logical infrastructure layouts of individual customer solutions. The complete history of customer service requests and incidents are recorded in the ticketing system. Customer-specific information is handled confidentially through permission-access levels in the ticketing system and access to customer infrastructures.

Documented procedures are in place for the monitoring of customer support operations against Service Level Agreement (SLA) guidelines. Internal Operational Level Agreements (OLAs) are followed in order to support customer SLAs and help ensure that identified issues are resolved. Furthermore, volume analysis, response times, and procedural adherence are monitored by support services quality analysts to help ensure designated SLAs are met. The OC management hierarchy is further responsible for the quality and service CenturyLink customers receive. Weekly and monthly key performance indicator reporting are utilized for performance management of the OCs.

Infrastructure

Electronic access systems, including badge and biometric access systems, are in place to restrict access to the data center facilities. The badge access system includes a monitoring and alerting console to notify onsite and local security operations personnel of activity and potential security violations. The ability to access the electronic access systems is limited to authorized security operations personnel. A building management system (BMS) is in place at most data centers to monitor environmental controls and alert data center staff to potential issues. The BMS has multiple access levels and passwords to restrict user access.

Remedy is the ticketing system/CRM system used centrally by CenturyLink to record and track customer requests and incidents from creation/identification to resolution. Remedy utilizes access levels and passwords to restrict user access within the respective ticketing system.
Various information systems are utilized to communicate information to customers and employees, as necessary. Monitoring systems are configured to log events and notify CenturyLink personnel of any exceptions. Detected customer-affecting issues are communicated to designated customer contact(s) via e-mail.

**Functional Areas of Operations**

The colocation services provided by CenturyLink are supported by the following functional areas:

- Executive management – responsible for overseeing company-wide activities, establishing and accomplishing goals, and overseeing objectives
- Security – responsible for the physical security of the data center facilities
- Facilities and engineering – responsible for the environmental security equipment at the data center facilities and supporting the media handling procedures
- Compliance management – responsible for monitoring services provided and ensuring compliance with internal service level agreements, external / customer commitments, and regulatory requirements
- Human resources (HR) – responsible for managing internal employee related issues and performing hiring and separation functions such as employee screening and termination procedures

**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 above and customer requests are recorded and tracked within the ticketing system.

The scope of this report is limited to the colocation services provided by CenturyLink. The colocation services include the physical infrastructure, power and data connectivity needed to house information systems of user entities. CenturyLink provides certain physical and environmental security as well as media handling mechanisms to safeguard user entities’ assets and data from unauthorized access and environmental threats.

Additional information regarding the description of the physical and environmental security and the media handling control activities are described in the Control Objectives and Related Control Activities section below. The specific control objectives can be found in Section 4 of this report along with the control activities and tests of operating effectiveness.

This report addresses internal controls in operation to support the CenturyLink data center facilities listed below.

<table>
<thead>
<tr>
<th>Site</th>
<th>Region</th>
<th>City/State</th>
<th>Site</th>
<th>Region</th>
<th>City/State</th>
</tr>
</thead>
<tbody>
<tr>
<td>AB3</td>
<td>USA</td>
<td>Albuquerque, NM</td>
<td>CL1</td>
<td>USA</td>
<td>Lewis Center, OH</td>
</tr>
<tr>
<td>AT1</td>
<td>USA</td>
<td>Lithia Springs, GA</td>
<td>PH1</td>
<td>USA</td>
<td>Phoenix, AZ</td>
</tr>
<tr>
<td>BO1</td>
<td>USA</td>
<td>Waltham, MA</td>
<td>PH2</td>
<td>USA</td>
<td>Scottsdale, AZ</td>
</tr>
<tr>
<td>BO2</td>
<td>USA</td>
<td>Waltham, MA</td>
<td>SC4</td>
<td>USA</td>
<td>Santa Clara, CA</td>
</tr>
<tr>
<td>BO3</td>
<td>USA</td>
<td>Waltham, MA</td>
<td>SC5</td>
<td>USA</td>
<td>Santa Clara, CA</td>
</tr>
<tr>
<td>CH2</td>
<td>USA</td>
<td>Chicago, IL</td>
<td>SC8</td>
<td>USA</td>
<td>Santa Clara, CA</td>
</tr>
<tr>
<td>CH3</td>
<td>USA</td>
<td>Elk Grove, IL</td>
<td>SC9</td>
<td>USA</td>
<td>Santa Clara, CA</td>
</tr>
<tr>
<td>Site</td>
<td>Region</td>
<td>City/State</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>--------</td>
<td>-------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CH4</td>
<td>USA</td>
<td>Chicago, IL</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DL1</td>
<td>USA</td>
<td>Dallas, TX</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DL2</td>
<td>USA</td>
<td>Dallas, TX</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DC2</td>
<td>USA</td>
<td>Sterling, VA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DC3</td>
<td>USA</td>
<td>Sterling, VA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DC4</td>
<td>USA</td>
<td>Sterling, VA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DC5</td>
<td>USA</td>
<td>Sterling, VA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DC6</td>
<td>USA</td>
<td>Sterling, VA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DC7</td>
<td>USA</td>
<td>Sterling, VA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DN1</td>
<td>USA</td>
<td>Highlands Ranch, CO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DN2</td>
<td>USA</td>
<td>Highlands Ranch, CO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DN3</td>
<td>USA</td>
<td>Englewood, CO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SL1</td>
<td>USA</td>
<td>Hazelwood, MO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BR1</td>
<td>USA</td>
<td>Burbank, CA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LA1</td>
<td>USA</td>
<td>El Segundo, CA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OC2</td>
<td>USA</td>
<td>Irvine, CA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MP1</td>
<td>USA</td>
<td>Minneapolis, MN</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MP2</td>
<td>USA</td>
<td>Minneapolis, MN</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NJ1</td>
<td>USA</td>
<td>Jersey City, NJ</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NJ2</td>
<td>USA</td>
<td>Weehawken, NJ</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NJ2x</td>
<td>USA</td>
<td>Weehawken, NJ</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NJ3</td>
<td>USA</td>
<td>Piscataway, NJ</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NJ4</td>
<td>USA</td>
<td>Piscataway, NJ</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NJ5</td>
<td>USA</td>
<td>Newark, NJ</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Site</th>
<th>Region</th>
<th>City/State</th>
</tr>
</thead>
<tbody>
<tr>
<td>SN1</td>
<td>USA</td>
<td>Sunnyvale, CA</td>
</tr>
<tr>
<td>SN2</td>
<td>USA</td>
<td>Sunnyvale, CA</td>
</tr>
<tr>
<td>SE2</td>
<td>USA</td>
<td>Tukwila, WA</td>
</tr>
<tr>
<td>SE3</td>
<td>USA</td>
<td>Tukwila, WA</td>
</tr>
<tr>
<td>SE4</td>
<td>USA</td>
<td>Tukwila, WA</td>
</tr>
<tr>
<td>TP1</td>
<td>USA</td>
<td>Tampa, FL</td>
</tr>
<tr>
<td>MR1</td>
<td>Canada</td>
<td>Verdun, QC</td>
</tr>
<tr>
<td>TR1</td>
<td>Canada</td>
<td>Mississauga, Ontario</td>
</tr>
<tr>
<td>TR3</td>
<td>Canada</td>
<td>Markham, Ontario</td>
</tr>
<tr>
<td>VC1</td>
<td>Canada</td>
<td>Vancouver, BC</td>
</tr>
<tr>
<td>LO1</td>
<td>UK</td>
<td>Berkshire, England</td>
</tr>
<tr>
<td>LO3</td>
<td>UK</td>
<td>London, England</td>
</tr>
<tr>
<td>LO4</td>
<td>UK</td>
<td>London, England</td>
</tr>
<tr>
<td>LO5</td>
<td>UK</td>
<td>Berkshire, England</td>
</tr>
<tr>
<td>LO6</td>
<td>UK</td>
<td>Berkshire, England</td>
</tr>
<tr>
<td>FR6</td>
<td>Germany</td>
<td>Frankfurt, Germany</td>
</tr>
<tr>
<td>BLR2</td>
<td>India</td>
<td>Whitefield, Bangalore, India</td>
</tr>
<tr>
<td>HK2</td>
<td>Asia</td>
<td>Hong Kong</td>
</tr>
<tr>
<td>SG2</td>
<td>Asia</td>
<td>Jurong East, Singapore</td>
</tr>
<tr>
<td>SG8</td>
<td>Asia</td>
<td>Singapore</td>
</tr>
<tr>
<td>TY6</td>
<td>Asia</td>
<td>Tokyo, Japan</td>
</tr>
</tbody>
</table>

Subservice Organizations

No subservice organizations were included in the scope of this assessment, including the colocation and building facility management support services provided for the data centers housed in third party buildings. The responsibilities of CenturyLink and the third party building management companies differ by location – for BLR2, FR6, PH1, PH2, SL1, and TY6, CenturyLink utilizes aspects of security services provided by the building management companies and the facilities / environmental equipment is owned and managed by the building management companies; for CH4, LO4 and MR1, CenturyLink utilizes the facilities / environmental equipment owned and managed by the building management companies, but the security services are the responsibility of CenturyLink.

For those data centers where the security services are provided by the building management companies (BLR2, FR6, PH1, PH2, SL1, and TY6), the building management companies are responsible for providing certain physical security controls, including controlling building access, access mechanisms and security monitoring via the electronic access system and/or surveillance camera system, to complement the security controls managed by CenturyLink. However, CenturyLink provides security access and monitoring systems for their space within data centers. For the data centers where the facilities / environmental equipment is owned and managed by the building management companies (BLR2, FR6, PH1, PH2, SL1, TY6, CH4, LO4, and MR1), the building management companies are responsible for providing environmental security safeguards to help ensure...
CenturyLink equipment is protected from certain environmental security threats such as fire, temperature and humidity levels, and loss of power. These companies are responsible for the maintenance and operation of environmental systems.

CenturyLink oversees and monitors the building management relationships to ensure that agreed service levels are being met.

**Significant Changes During the Review Period**

During the review period, CenturyLink discontinued service operations to the MP1 datacenter. This discontinuance of service for the aforementioned datacenter was completed on June 25, 2016. No other significant changes during the review period were noted.

---

**CONTROL ENVIRONMENT**

CenturyLink’s internal controls are a set of processes and procedures with oversight by its board of directors, executive management team and other personnel in order to provide reasonable assurance regarding the achievement of CenturyLink’s objectives in the following categories: (a) reliability of financial reporting, (b) effectiveness and efficiency of operations, (c) compliance, and (d) customer service and support. The following is a description of the five components of internal control for CenturyLink: control environment, risk assessment, control objectives and related control activities, information and communication systems and monitoring.

**Integrity and Ethical Values**

CenturyLink as a whole, including its data centers and IT environment has programs and policies designed to promote integrity and ethical values in its various environments. CenturyLink maintains a documented code of conduct. Employees are required to acknowledge that they have been given access to the employee policies and procedures and understand their responsibility for adhering to them. Additionally, employees have access to review the code of conduct throughout the year as it is maintained on CenturyLink’s corporate intranet.

CenturyLink has established companywide security policies for its corporate and data center facilities. CenturyLink requires adherence to the security policies and conducts periodic seminars and/or distributes information in order to support a culture of integrity and ethics. In addition to ad hoc sessions, company training calendars, and CenturyLink e-mails (internal newsletters) are maintained on the corporate intranet, inviting personnel to attend the training session(s), and employees are required to undergo security awareness training on an annual basis.

Employees are required to acknowledge that they have been given access to the code of conduct which includes the confidentiality statement and agree not to disclose proprietary or confidential information, including client information, to unauthorized parties.

**Board of Directors and Audit Committee Oversight**

CenturyLink’s board of directors provides oversight to executive management. CenturyLink executive management recognizes its responsibility for directing and controlling operations and for establishing, communicating, and monitoring control policies and procedures. Corporate and operating unit management are responsible to executive management for establishing and maintaining internal controls and promoting integrity and ethical values to CenturyLink personnel.

CenturyLink’s commitment to an effective system of internal controls starts with the existence of CenturyLink’s audit committee. The audit committee is responsible for the appointment, compensation, retention, and oversight of the work of any registered public accounting firm employed by CenturyLink to assist the board of directors oversight of (1) the accounting and financial reporting process of CenturyLink, which includes certain financial information supplied by CenturyLink in connection with the audit of the financial statements of CenturyLink, (2) the
qualifications and independence of CenturyLink’s independent auditor, and (3) the performance of CenturyLink’s internal audit functions and independent auditors specific to CenturyLink operations. The audit committee, which is made up of independent directors, meets at least once per quarter.

CenturyLink’s corporate operations include the internal audit department whose mission is to provide independent, objective assurance and consulting activities designed to add value and improve CenturyLink’s operations. The scope of its charter is to determine whether CenturyLink’s network of risk management, control, and governance processes, as designed and represented by management, is adequate and functioning as intended for all business units, which includes CenturyLink operations. The purpose of the internal audit department includes (1) helping to ensure management has implemented internal controls, (2) advising business unit management regarding risks and helping management identify controls to mitigate the risks, and (3) assessing the controls and operations within business units and reporting the results of the assessments to management and the audit committee.

Organizational Structure and Assignment of Authority and Responsibility

The organizational structure of CenturyLink, which provides the overall framework for planning, directing, and controlling operations, uses an approach whereby personnel and business functions are divided among department units according to job responsibilities and work requirements. This approach allows the organization to better define responsibilities, lines of reporting, and communications allowing employees to focus on relevant business issues.

Organizational charts and job descriptions for each area owner within the data centers and the IT environment have been implemented and are posted on the corporate intranet.

Commitment to Competence

CenturyLink’s management has determined the competency levels required for the various personnel who staff data centers and the IT environment. HR has a team dedicated to ongoing employee training. CenturyLink maintains a learning system on the corporate intranet where employees can obtain additional skills training in order to help perform their job responsibilities effectively. The employees’ job responsibilities are also reinforced through on-the-job training. CenturyLink e-mails are also sent to highlight upcoming training events.

New employees typically participate in an orientation program with their direct management, introducing them to CenturyLink’s processes and functions, as well as job-specific training.

Accountability

Management’s Philosophy and Operating Style

CenturyLink has developed various policies designed to provide corporate oversight. Such policies have been issued and posted on the corporate intranet and communicated to employees through CenturyLink e-mails. CenturyLink has a corporate compliance officer that oversees CenturyLink’s corporate compliance programs. CenturyLink has a whistle-blower policy on the corporate intranet for employees to express, confidentially and anonymously, concerns they may have to independent members of CenturyLink’s corporate compliance team made up of members of the legal staff.

Hiring Practices

CenturyLink has implemented formal hiring practices that are designed to help ensure that new employees are qualified for their job responsibilities. This includes an overview of the job description that the manager is required to discuss with new hires. Applicants are subject to an interview process that assesses their qualifications related to the expected responsibility level of the individual and CenturyLink leadership model. Consistent with applicable law, employees must successfully pass a pre-employment screening process that includes, depending upon the location, past employment history, a criminal background check, and a drug/controlled substances check. A standardized ticket or form is completed for new employees to guide the onboarding process.
CenturyLink data centers and the IT environment employ personnel training to help maintain the skill levels and competencies of personnel.

**Termination Practices**

CenturyLink’s HR department has defined termination policies for both voluntary and involuntary termination of employment. Employment with CenturyLink is at will and may be terminated at any time, for any reason, by either CenturyLink or the employee.

At its discretion, and in accordance with applicable laws, CenturyLink reserves the right to terminate employment of any employee at any time when it considers the termination to be in the best interest of the Company. Reasons for involuntary termination include, but are not limited to, reduction in force (RIF), lack of work, misconduct, violation of company policy, performance that does not meet the expectations of CenturyLink, misrepresentation on employment application, insubordination, and any violation of local, state, or federal law when conducting business on behalf of CenturyLink.

A standardized ticket or form is completed for terminated employees to guide the termination process and help ensure that out-processing procedures are performed.

---

**RISK ASSESSMENT**

**Risk Identification and Analysis**

CenturyLink data centers and corporate environments are subject to a comprehensive audit program managed by the corporate information security, internal audit and compliance management departments. The internal audit department performs periodic audits of CenturyLink’s operational and/or business functions and, on an ongoing basis, facilitates testing of the company’s key Sarbanes-Oxley controls as a part of management’s assessment of its control environment.

Compliance Management also supports internal testing of select security and compliance-related controls including reviews to assess whether the data centers are conforming to company security and access procedures and to validate adherence with the control objectives of the annual SSAE 16 / ISAE 3402 examination. Compliance Management develops an audit plan for CenturyLink data centers based on prior audit results and management input.

Senior leadership including, but not limited to, the senior vice president of global operations and product, and the functional heads of the engineering, development, and operations departments, is responsible for overall risk assessment and policy maintenance, as deemed necessary. The information security group also facilitates periodic executive management reviews to provide insight and guidance relative to overall corporate information security risk posture.

**Risk Factors**

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

**External Factors**

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

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

Risk Analysis

CenturyLink’s management has placed into operation a risk assessment process to identify and manage risks that could affect the organization's ability to provide colocation services for user entities. These risks and the associated measures to help mitigate the risks are described below.

Physical security risks have been considered and include, but are not limited to, the following:

- Non-authorized individuals will enter the raised floor of the data center (visitors, customers, contractors or employees)
- Individuals entering the data center may not be who they say they are
- Terminated employees and contractors will be able to enter the data center
- Temporary badges or loaner keys would be lost or taken

In order to address physical security related risks, policies and procedures are in place and utilized by each data center. The CenturyLink Technology Solutions Global Physical Security Policy is used for the United States, United Kingdom, Singapore and Canadian data centers. Tokyo and India have individual procedures depending on necessary actions taken.

Risks related to facilities and environmental protection have been considered and include, but are not limited to, the following:

- Consistent levels of environmental protection are not maintained across the data centers
- The correct equipment is not in place at each data center
- Systems are not monitored
- Equipment does not run properly or when needed
- Inadequate power or fire suppression

In order to address facility and environmental protection related risks, each data center follows a policy on the acceptable conditions and handling of the facilities and environment of the data center. Additionally, a BMS is used for data center equipment to help ensure alerts are sent out when equipment is not properly functioning. If issues are identified, they are noted and repaired. Quarterly, semi-annual and annual maintenances are performed on equipment within each data center whether owned by CenturyLink or a third party.

CenturyLink has considered the following risks related to media handling services:

- Media is transferred or recalled by unauthorized individuals
- Media handling activities are not performed in accordance with predefined schedules
- Media handling activities are not performed in accordance with customer directives
In order to address risks related to the media handling services, there is a process by which each data center has authorized individuals who can pull tapes from the backup equipment when a work order is received internally. The tapes are stored in a restricted and secured area until the third party vendor arrives. The third party vendor verifies the person handing over the tapes is authorized to do so and transports the tapes to their facility for secure storage. CenturyLink maintains a list of individuals authorized to request media from the third party vendor.

Integration with Control Objectives

Risk identification establishes the exposure of the organization to risk and uncertainty. The results of the risk analysis are used to produce a risk profile that gives a rating of significance to each risk and provides a tool for prioritizing risk treatment efforts. The results are then ranked based on relative importance of each identified risk.

The SSAE16 program is integrated with the Global CenturyLink Risk/Threat Framework. This will include knowledge of the factors critical to success and the threats and opportunities related to the achievement of the SSAE16 objectives. Along with assessing risks, management has identified and put into effect actions needed to address those risks. In order to address risks, control objectives have been defined for each significant risk area. Control activities are then defined to serve as mechanisms for managing the achievement of those objectives and help ensure that the actions associated with those risks are carried out properly and efficiently.

CONTROL OBJECTIVES AND RELATED CONTROL ACTIVITIES

Selection and Development of Control Activities

Control activities are a part of the process by which CenturyLink strives to achieve its business objectives. CenturyLink 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 CenturyLink evaluate the relationships between business processes and the use technology to perform those processes to determine the dependencies on technology. The security management processes for the technology, along with other factors, are analyzed to define and establish the necessary control activities to achieve control objectives that include technology. The establishment of the control activities is enforced by defined policies and procedures that specifically state management’s directives for CenturyLink 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.

CenturyLink’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.

Physical Security

Control Objective: Control activities provide reasonable assurance that CenturyLink’s data centers, system and network equipment, and storage media are protected from unauthorized access.
Organization


The Global Data Center Physical Security group manages all aspects of the physical security of the CenturyLink data centers, including the security policies and procedures, security officer staffing, access control systems (ACS), video surveillance systems, standards compliance, and physical security designs and improvements within the data centers. Data centers have a security operations center (SOC) or security desk. Data Center Security personnel control data center access, monitor local security alarms and CCTV cameras, and manage physical security-related issues from the SOC.

The Physical Security group establishes security policies for all other CenturyLink facilities, manages Company ACS, and coordinates security improvements to CenturyLink properties. The Physical Security team manages the Corporate Security Operations Center (CSOC), the Central Access Command Center (CACC) and provides technical engineering support for CenturyLink security access control and CCTV systems.

Physical Security Controls

CenturyLink employs a variety of physical security measures to provide the level of security necessary based on the type of site. Data Center Security Operations and the Physical Security - Engineering staff monitor and research the physical security industry and meet with the engineering and technical staff of leading manufacturers to ensure the sites remain up-to-date. CenturyLink relies upon CCTV surveillance; computer-based access control/alarm systems, biometric readers, restricted key systems, ballistic protections and exterior perimeter controls in its multi-layered physical security program. The mix of physical security hardware is dependent upon the unique characteristics of the facility (single versus multi-tenant; owned versus leased; single versus multi-floor; etc.), uses of the facility (data center, administrative offices, etc.), age and design generation of the facility as well as the geographic location.

Portals and mantraps are used at the main access point beyond the front lobby or to a Restricted Area and are specifically designed to prevent tailgating and piggybacking attempts. Entry into the portal or mantrap requires card reader access. Only one person may be inside the portal or man trap at a time. Once inside the portal or mantrap, exit into the secure area of the data center requires two factor authentication of the cardholder using a biometric reader. Exiting the secure area of the data center through the portal or mantrap requires card reader access. Only one person may enter the portal or mantrap at a time. Free egress will occur once the secure-side door is in a closed position. In data centers without portals or mantraps, the security officer monitors the entrance to prevent tailgating.

Where present, a portal by-pass door is specifically designed to be used to “by-pass” a mechanical portal in the event of a mechanical failure or emergency, or the need to move items deemed too large to fit through the portal. The by-pass door should be used only as an emergency entrance or exit. CenturyLink customers and contractors may not have permanent badge access to by-pass doors. Exceptions for individuals who are unable to use the portal due to disability, phobia or other restrictions must be submitted and approved on a badge request. Temporary badge access to by-pass doors will be granted by Data Center Security Operations to all badge holders in the data center while a portal is in a failure mode and not available. Data Center Security Operations personnel may allow escorted visitors and large group tours to use the by-pass door.

CenturyLink uses an ACS and access badges to restrict access within data centers to only those individuals with proper authorization. CenturyLink access badges provide access authorization to CenturyLink facilities and are used for gaining entry into controlled areas within those facilities. CenturyLink access badges are issued to authorized individuals and are for their sole use only. The sharing of badges or personal identification number (PIN) codes between individuals for any purpose whatsoever is strictly prohibited The ACS is used to monitor, log, and notify personnel of security alarms. The ACS is equipped and programmed to receive alarms for forced doors, propped doors, and denied card reader attempts. The ACS monitors perimeter doors, elevators where applicable, restricted area doors, shipping and receiving doors and customized access control doors and devices for customers.

All access control records and the system on-line event database reporting must be available online for 90 days. Events beyond 90 days must be archived and stored offline for a minimum of two years. Any cardholder profile with a history of access is retained in the online database for a minimum of two years. This data consists of the
cardholder full name and company name as well as their access history. Biometric readers perform dual-authentication of an access cardholder as an added access security measure.

CenturyLink utilizes CCTV surveillance in all data centers 24 hours daily. All CCTV components are installed to monitor live and recorded footage. Interior CCTV cameras are to be positioned throughout the data center to enable CenturyLink to track and monitor the activity of any person while inside the data center. Interior cameras are positioned to monitor perimeter doors, data center main entry/exit, data center raised floor entry/exit, cage aisle ways, shipping and receiving areas, high-security vaults, and other areas. The interior raised floor area must have a dedicated camera at all doors placed to capture facial recognition on entry to the raised floor. All raised floor perimeters and aisle ways must have CCTV coverage.

Exterior cameras are positioned to provide views of support equipment, perimeter doors, and parking areas, where applicable. The full exterior perimeter of the building is covered with a mixture of Pan-Tilt-Zoom (PTZ) and fixed exterior cameras. Shipping and receiving loading dock areas are required to have either a fixed dedicated exterior cameras or PTZ covering all loading bay doors. Shipping and receiving and secured storage areas are required to have interior camera coverage. Cameras record activity on-site via network or digital video recorders. All interior cameras on the raised floor and secure areas of the datacenter are required to meet the specification of 90 day retention of recorded footage.

All security systems have dedicated UPS systems and standby emergency power (SEP) support (i.e., generators).

The SOC is the primary security and access control operation for CenturyLink data centers. The SOC is used to monitor and control access and security alarms and monitor the CCTV cameras and where all related security operational activities occur 24 hours a day, 7 days a week. The SOC is a highly restricted area within the data center facing the front main entrance lobby. As such the SOC construction should consist of UL rated, Level 3 ballistic protection in the walls and window glass facing the outer front lobby. The SOC is serviced by UPS (battery support) and stand-by electrical power (electrical generator) support for continuous operation of communications, lighting, CCTV, intrusion detection and alarm monitoring equipment in the event utility power loss. The entrance to the SOC is from the restricted area of the data center, where possible, and should have a minimum of card reader access.

Customer equipment is physically secured within locked cages, cabinets, or vaults. The Data Center Security Operations personnel act as custodians of customer loaner and backup cage keys, which are maintained in the SOC or similar secured area. They also administer temporary PINs for access to cages, as needed. The listing of customers, customer employees, and cage, cabinet, and vault assignments are updated in real time to help ensure access is limited to authorized personnel. Customer loaner and backup cage keys are tracked by CenturyLink through an issue, track, retrieval, and audit storage process.

Data Center Security Operations

Each data center has a SOC or security desk. Data Center Security Operations personnel work within the SOC to control data center access to ensure compliance with access procedures, administer the ACS to permit and terminate access to the data center, monitor security alarms for intrusions or unauthorized access, monitor CCTV camera images of activity within the data center to detect improper or unsafe acts, and manage all security-related issues from the SOC or security desk including issuing photo identification (ID) access badges and visitor badges, issuing metal cage loaner keys and retrieving the same. Data Center Security Operations personnel receive security training and certification prior to their full-time assignment within a data center and continuously thereafter. Data Center Security Operations personnel also maintain first aid, cardiopulmonary resuscitation (CPR) and automated external defibrillator (AED) training certifications.

The CSOC provides global, 24x7 support to the local data center security teams with remote monitoring, management, administration and maintenance of the ACS and CCTV video surveillance systems used throughout CenturyLink data centers. The CSOC also assists and directs local data center security in the response to predefined alarms, physical security incidents and events involving law enforcement, fire or emergency medical personnel. The CSOC is responsible for monitoring alarm events and continuous System Hardware Tree communication, mask and/or unmask readers, enable and/or restore IDC portal bypass, and trace badges, alarms, devices and controller events. The CSOC maintains the hardware equipment for security related devices on the CenturyLink ACS and is responsible for the system administration for the ACS. The CSOC is responsible
for remotely monitoring, investigating, and responding to alarm events identified as “critical” and not yet acknowledged by Local Data Center Security Operations within 20 minutes of alarm generation by the ACS. The CSOC is responsible for responding to and resolving all security related impairment reports from the data centers that impact the ACS, CCTV surveillance or other security-related systems.

The CACC within CenturyLink Corporate Security supports the distribution of all CenturyLink access badges and the administration of access permissions within the ACS. The CACC tracks the distribution of identification badges and maintains the hardware equipment for all security related devices. In addition, the CACC is responsible for the timely fulfillment of all badge requests. Additionally, physical access to the colocation facilities is revoked as a component of the termination process.

A Regional Security Manager (RSM) provide overall security support for the data centers within specified regions, assist with the development of policy and procedures and maintain oversight of SOC operations and security vendors to ensure compliance with policy and procedures is maintained.

The Manager – Physical Security – Global Data Center Physical Security is responsible for the overall physical security operation within the CenturyLink data centers, establishing policy and procedures, and ensuring policy and procedures are reviewed and updated as necessary on an annual basis.

Data Center Security Operations management conducts periodic audits to help ensure that security operations personnel are comprehending and following the data center policies and process, that security operations personnel are trained and annually certified on security policies and procedures, that daily key inventory and security rounds are performed, authorized access records are kept, and that the use and servicing of physical security hardware equipment is performed as needed.

Data Center Access

All persons are required to enter and exit the data center through the designated main entrance. CenturyLink Data Center Operations employees may use designated employee entrances other than the main entrance.

All persons requesting access to a CenturyLink data center must verify their identity by presenting valid government-issued photo ID or a CenturyLink-issued photo access badge. For those persons without a CenturyLink issued badge, a visitor log is utilized and maintained for at least 90 days to document the visit.

All persons entering the secured area of the data center are required to have a CenturyLink permanent, temporary or visitor access badge. Access badges are to be worn by the individual at, or above, the waist and be visible at all times. A badge request is required for all permanent CenturyLink access badges. All requests for badge access to CenturyLink data centers must be submitted and approved by the sponsor/manager and the designated Data Center Site Authorizer. All facility contractors or vendors must have an unexpired work order authorization issued by CenturyLink operations personnel to access a CenturyLink data center.

CenturyLink colocation customers may authorize physical access to any CenturyLink data center where they have active colocation services. CenturyLink colocation Customers are responsible to provide and maintain an accurate Access Authorization List listing of their employees, contractors and vendors requiring access into their colocation space within CenturyLink Data Centers.

Customers assign data center access authorization to an Active Contact on either a “Permanent” or “Temporary” basis. Customers and their authorized representatives will have unescorted access to the data center and their colocation space on a 24x7 basis, dependent upon local conditions. All persons listed as active contacts on the Customer Access Authorization List and authorized for “Permanent” access are eligible to request a permanent CenturyLink customer access badge. Persons authorized for “Temporary” access are provided a temporary customer badge while in the data center.

Customers and their authorized representatives may not enter Restricted Access Areas of the data center without escort by an authorized CenturyLink employee. Customers and their authorized representatives may not enter the Managed Service, Network Node, and Meet Me Room areas of the data center at any time.

Visitors must demonstrate a legitimate business purpose for visiting the site and must be escorted by an Authorized Sponsor while in the data center.
Shipment Management

Received CenturyLink and customer equipment is stored within the designated shipping and receiving area, or secured storage area, within each data center facility. Shipping and receiving and secured storage area access is limited to authorized personnel only. CenturyLink Data Center Security Operations, as well as shipment management personnel, monitor incoming and outgoing vehicles, where physically possible. CenturyLink shipment management personnel ensure that CenturyLink goods entering and leaving the premises are accompanied by duly completed documentation.

Incoming Shipments

Documented policies and procedures are in place to help ensure incoming shipments are handled correctly for both CenturyLink and customer equipment. Incoming shipments are only accepted if they are addressed to an authorized employee or customer of that particular CenturyLink location. Procedures have been established to detect suspicious packages or otherwise hazardous materials and to handle such items. If the item is deemed acceptable to the data center, shipment management personnel will perform a box count, log the shipment (including the tracking number) into the receiving log, and notify the validated employee or customer of the receipt for pickup. Further, customers are responsible for follow-up on shipments sent directly to a CenturyLink facility.

Data Center Assessments

The compliance program management team risk ranks each data center and performs on-site or remote reviews of each data center according to a predefined schedule based on risk ranking. Personnel document the reviews in a standardized data center assessment feedback template where findings and remediation steps are tracked.

Environmental Security

Control Objective: Control activities provide reasonable assurance that CenturyLink facilities housing customer equipment and support operations are protected from certain environmental threats (power loss, fire, temperature and humidity levels).

CenturyLink has developed environmental security policies and procedures to serve as a guide for personnel in areas that include, but are not limited to, equipment specifications and operating instructions, equipment inspections, and preventive maintenance schedules.

Data Center Infrastructure – The overriding criteria in the build of data centers are that critical mechanical and electrical components are designed with adequate redundancy. For example, the possibility that a system is shut down for maintenance and that a failure of another system component occurs at the same time is considered. In critical systems, N + 1, N + 25%, or, in some cases, 2N redundancy is provided.

Data center facilities meet applicable state and federal regulatory requirements for environmental health and safety, including written emergency response plans, emergency contacts notification, inventory of hazardous chemicals, personal protective equipment (PPE), chemical spill kits, and hazard communication/warning signage. Furthermore, data center space is kept clean of debris, and floors are maintained regularly. Food and drink are prohibited in the data center raised floor area.

Control and Monitoring Systems – A BMS is in place at the data center facilities. The BMS is a monitoring and reporting system used to monitor environmental controls and alert data center staff via e-mail and on-screen alerts to potential issues when predefined thresholds are met or exceeded.

The BMS monitors the following:

- Power systems, including critical electrical components: generators, transfer switch, main switchgear, power management module (PMM), and UPS equipment
- The HVAC system, which controls or monitors temperature and humidity within the data centers, space pressurization, HVAC equipment run status and performance, and outside air conditioners
- Fire detection and suppression systems
Procedures are in place to help ensure data centers have a consistent level of facility and environmental protection. Data center technicians perform and log regular equipment checks and maintenance procedures to ensure that fire detection and suppression, power management, including battery and fuel monitoring systems, and HVAC equipment are working properly. Furthermore, maintenance procedures are performed periodically by external vendors to test and validate the operation of power management equipment, fire detection and suppression equipment, HVAC equipment, and humidity, temperature, and water detection sensors. Service reports are provided by each vendor documenting the results of the maintenance.

**Fire Detection and Suppression** – Sprinkler systems in the data centers are implemented with double interlock pre-action and detection systems. The systems are designed such that water does not enter the sprinkler system piping during normal operations. Pre-action detection intelligent heat detectors are installed in the ceiling of mission-critical areas of each data center.

Upon activation of any of these heat detectors, audio-visual alarms (horn and/or strobes) will activate throughout the space. A signal will be sent to a pre-action valve for the affected fire zone. If the temperature in the at-risk area also reaches levels to melt any of the sprinkler head fusible links, water is triggered to enter the sprinkler pipes for the affected areas of the data center.

Fire extinguishers are provided throughout each data center. Dry chemical or clean agent extinguishers are installed in the mission-critical space or adjacent areas where one might reasonably expect a person to carry them into the affected areas during an emergency.

The fire suppression systems are monitored 24x7 by an external alarm monitoring company, which will dispatch the local fire department upon receipt of an alarm and/or confirmation of a fire (depending on local fire regulations). Inside the data centers, software is used for fire detection and monitoring, combined with customized floor plan graphics to illustrate detection devices and fire zones to aid data center personnel and the fire department in responding to and coordinating fire control activities. Third party specialists inspect the fire detection and suppression systems on an annual basis and perform preventative maintenance.

**Power Management: Utility and Backup Power** – Each data center is supplied with either medium or high voltage electrical power from the local utility company. Where possible, two independent utility sources are in place, originating from independent feeders or substations. Each data center is powered by a dedicated utility step-down transformer for each service. The incoming service is connected to an automatic transfer switch, which is also connected to redundant standby diesel generators.

Electrical loads served by the incoming service and generator sources include mission-critical, life safety, HVAC, and general-purpose loads. Third party specialists inspect the power management systems including, but not limited to, the UPS systems, power distribution units (PDUs), and generators on an annual basis and perform preventative maintenance.

**UPS Systems** – The mission-critical electrical loads at each data center are sourced by redundant UPS systems which are configured with automatic static-bypass and manually operated full-maintenance bypass circuits. The primary UPS system consists of online, stand-alone modules providing conditioned, uninterruptible power to critical electrical loads. Distributed redundancy is achieved through a reserve UPS system.

**PMMs/ PDUs** – CenturyLink makes use of PMMs and PDUs on data center raised floors to provide for a physically integrated and electrically redundant system for source selection, isolation, distribution, monitoring, and control of power to internal and customer computer loads.

**Generators** – CenturyLink has diesel engine generators in place at each data center to provide power to critical equipment and customer loads. Generators may be located indoors or outdoors, depending on site-specific conditions. Base tanks or “day tanks” provide up to 3,000 gallons of fuel storage. Separately installed main fuel tanks provide a source of fuel to engine-generators. There is fuel storage on-site sufficient for at least 12 hours of design load operation, or as much fuel as local authorities will allow. Generator backup capabilities at each data center include a short-notice refueling contract for the diesel generators.

**HVAC** – Each data center is built with zoned temperature control systems. CenturyLink maintains multiple HVAC units at each data center to verify correct temperature in critical areas. The average temperature within each zone is maintained between 65° and 80° Fahrenheit, as required for the area. If the temperature varies outside
early-warning, preset sensitivity limits, an alarm is generated in the NOC area, and facilities personnel are notified. The HVAC units are also powered by both normal and emergency electrical systems for redundancy. Third party specialists inspect the HVAC systems on an annual basis and perform preventative maintenance.

Data Center Assessments
The compliance program management team risk ranks each data center and performs on-site or remote reviews of each data center according to a predefined schedule based on risk ranking. Personnel document the reviews in a standardized data center assessment feedback template where findings and remediation steps are tracked.

Media Handling
Control Objective: Control activities provide reasonable assurance that CenturyLink and customer backup media is secured, tracked and access to backup media is limited to authorized individuals.

CenturyLink offers various services to support customers’ backup and restore needs. Experienced backup engineers with relevant training and experience work together to support the customers’ needs and help to ensure backups are run and complete successfully.

Policies and procedures are in place to support the administration of CenturyLink’s managed backup services. Administrative access to the backup schedules is limited to engineers or hosting operations personnel (Tokyo, Japan) through the use of individual user accounts with unique identifiers. The various backup systems can only be accessed through SSH authentication.

CenturyLink currently provides variations of backup and restore services:

- Utility backup service
- Utility backup encryption service
- Utility backup NAS service
- Utility vaulting service

Utility Backup includes data backup and restore on demand, utilizing high-capacity and high-availability tape libraries. Utility Backup Encryption provides the same services as Utility Backup with the addition of data encryption throughout the lifecycle of the data. Utility Backup NAS provides similar services to Utility Backup, utilizing technologies (such as Network Data Management Protocol (NDMP) designed specifically for NAS-based data. Utility Vaulting includes retention, data management, and rotation of data to off-site secure data archiving facilities.

Standard backup services provide daily incremental and weekly full backups for customers and are retained according to the individual customer’s corresponding SLA in either the tape library or virtual tape library. For Utility Vaulting customers, backup tapes are rotated on a predetermined or as-needed basis to CenturyLink’s contracted third party storage provider. Off-site backup tapes can be monitored by the backup services team online.

Managed backup systems are monitored 24x7 by the CenturyLink OC using the automated monitoring tool. An alert is sent to the automated monitoring tool database if a backup failure cannot be restarted after three attempts by the backup agent. The OC will document the issue/failure in a service ticket in the ticketing system and attempt to restart the backup manually. If the OC cannot restart the backup, the service ticket will be escalated to the Managed Storage Operations (MSO) team for follow up and resolution.
INFORMATION AND COMMUNICATION SYSTEMS

Relevant Information

Information is necessary for CenturyLink 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 electronic access systems, including badge and biometric access systems, are 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 surveillance camera systems are used to monitor and record activity at the data center facilities.
- The BMS provide alerts and reporting regarding the environmental security equipment at the data center facilities.
- E-mail and the Vantive ticketing system are used to communicate with internal and external / customer personnel regarding services provided, requested, queries, and potential events or incidents identified.

Communication

CenturyLink has implemented various methods of communication to help employees understand their roles and responsibilities and to communicate significant events. The methods of communication include e-mail, intranet postings, department telephone trees, etc. Management teams also hold regular staff meetings to track project status and receive updates, as necessary.

E-mail is one preferred method of communication for CenturyLink employees for time-sensitive information. CenturyLink has also implemented an automated call-system, OneCallNow.com, which is used to notify responsible parties of critical system events that require immediate attention, including but not limited to executive management.

MONITORING

Monitoring Activities

CenturyLink employs various tools, technologies, and procedures to monitor and evaluate the operational effectiveness of internal controls around the services which CenturyLink provides both to its internal users and to its external customers. Documented procedures are in place to facilitate the monitoring of CenturyLink and customer systems.

CenturyLink has implemented the Customer Care Forum (CCF), which monitors critical service-impacting issues and events which affect CenturyLink customers. The CCF holds daily operational calls to discuss these areas of concern, as well as potential issues pertaining to internal control and process improvement opportunities. Any changes to internal controls recommended by the CCF calls are presented to management for review and approval.

Data center facilities employ several layers of monitoring. Data center facilities are monitored by security cameras on a 24x7 basis. CenturyLink’s physical ACS also monitors points of ingress and egress for each data center, notifying security operations personnel of any alarms generated by the system. There is also a BMS in place at applicable data centers which monitors the environmental controls for each facility, including HVAC, fire
detection and suppression; and power management equipment. The BMS promptly notifies the on-call facilities engineer(s) for the corresponding data center and the local security operations personnel of any system alarms. In addition, the Compliance Management organization conducts assessments of the data centers according to a predefined schedule based on risk ranking to ensure control objectives are still effective.

The various monitoring systems also generate management reports in order to review system performance and trends. Management reviews these reports in order to facilitate the resolution of issues and make sure that corrective actions are taken. CenturyLink also reviews monthly and quarterly metrics.

**Internal Auditing**

Management performs routine checks via process verification and reporting to ensure that policies and procedures are being followed. Management also conducts monthly operational meetings to review statistics and discuss issues and remediation. Additionally, managers and supervisors are hands-on and in constant contact with employees to help ensure processes and procedures are continually improved. Regional and global management teams maintain communication to identify and resolve issues that arise.

Differences exist regionally; however, management performs routine checks on data center processes to help ensure policies and procedures are followed. For example, to ensure compliance with physical security controls, CenturyLink uses multiple methods to verify internal controls are followed, including, but not limited to, training, testing, auditing, troubleshooting, and site visits. To ensure compliance with facility and environmental protection controls, equipment is inspected by internal personnel and third party specialists to help ensure systems are functioning properly. Managers conduct random audits and site visits/surveys. Documentation is reviewed monthly and site visits are conducted according to a predefined schedule based on risk ranking. Additionally, managers and supervisors are hands-on and in constant contact with employees to help ensure processes and procedures are continually improved. Regional and global management teams maintain communication to identify and resolve issues that arise.

**Reporting Deficiencies**

Management has developed protocols to ensure findings of internal control deficiencies should be reported not only to the individual responsible for the function or activity involved, who is in the position to take corrective action, but also to at least one level of management above the directly responsible person. This process enables support or oversight for taking corrective action, and to communicate with others in the organization whose activities may be affected. Any deficiencies found via the ongoing monitoring activities are further investigated by CenturyLink’s compliance department and members of the management team, as applicable. Deficiencies are tracked from identification to resolution.

For example, for physical security and facilities controls, incident reports and impairment reports are utilized to note any deficiencies. Incident reports take care of any process issues and findings. Impairment reports are logged for equipment failures or needs. Incident and Impairment reports are reviewed by management to see if processes and procedures are effective. Any issues stemming from the reports are remediated and reviewed by management. If issues cannot be resolved, they are escalated to upper management based on policies and procedures.

**Complementary Controls at User Entities**

CenturyLink’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 CenturyLink’s colocation services system to be solely achieved by CenturyLink’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 CenturyLink.
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:

**Physical Security**

1. User entities are responsible for reading and adhering to the terms and conditions of the CenturyLink master service agreement and CenturyLink rules and regulations regarding conduct in the data centers.

2. User entities are responsible for maintaining their own asset control processes and policies and for insuring their equipment housed within the CenturyLink data centers.

3. User entities are responsible for notifying CenturyLink of changes to their incident response policy and procedures, including points of contact.

4. User entities are responsible for notifying CenturyLink of on-site visits of employees, vendors and contractors prior to their arrival to the data center(s).

5. User entities are responsible for adhering to the CenturyLink physical security and safety procedures.

6. User entities are responsible for informing their vendors of the CenturyLink security procedures.

7. User entities are responsible for ensuring their guests/visitors are escorted, as appropriate, throughout the CenturyLink data centers.

8. User entities are responsible for providing CenturyLink the listing of individuals authorized to access the data center and customer cage, and for notifying CenturyLink 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.

10. User entities are responsible for developing policies and procedures to protect their systems from unauthorized or unintentional use, modification, addition, or deletion.

**Media Handling**

11. User entities are responsible for establishing procedures to help ensure data is backed up, or the user entity must contract with CenturyLink to perform these services, in accordance with CenturyLink’s standard procedures and applicable charges.

12. User entities are responsible for ensuring that data and content are lawful and do not violate any applicable laws and/or regulations.

13. User entities are responsible for the accuracy and integrity of the data backed up by the CenturyLink Managed Backup service.
SECTION 4

TESTING MATRICES
Scope of Testing

This report on the controls relates to the Colocation Services system provided by CenturyLink. The scope of the testing was restricted to the Colocation Services system considered to be relevant to the internal control over financial reporting of respective user entities. Schellman & Company, LLC conducted the examination testing over the period July 1, 2015, through June 30, 2016.

Tests of Operating Effectiveness

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

<table>
<thead>
<tr>
<th>Test Approach</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inquiry</td>
<td>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.</td>
</tr>
<tr>
<td>Observation</td>
<td>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.</td>
</tr>
<tr>
<td>Inspection</td>
<td>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.).</td>
</tr>
</tbody>
</table>

Sampling

Consistent with American Institute of Certified Public Accountants (AICPA) authoritative literature, Schellman & Company, LLC utilizes professional judgment to consider the tolerable deviation rate, the expected deviation rate, the audit risk, the characteristics of the population, and other factors, in order to determine the number of items to be selected in a sample for a particular test. Schellman & Company, LLC, in accordance with AICPA authoritative literature, selected samples in such a way that the samples were expected to be representative of the population. This included judgmental selection methods, where applicable, to ensure representative samples were obtained.
System-generated population listings were obtained whenever possible to ensure completeness prior to selecting samples. In some instances, full populations were tested in cases including but not limited to, the uniqueness of the event or low overall population size.

Test Results

The results of each test applied are listed alongside each respective test applied within the Testing Matrices. Test results not deemed as control deviations are noted by the phrase “No exceptions noted.” in the test result column of the Testing Matrices. Any phrase other than the aforementioned, constitutes a test result that is the result of non-occurrence, a change in the application of the control activity, or a deficiency in the operating effectiveness of the control activity. Testing deviations identified within the Testing Matrices are not necessarily weaknesses in the total system of controls at user entities, as this determination can only be made after consideration of controls in place at user entities, and other factors. Control considerations that should be implemented by user entities in order to complement the control activities and achieve the stated control objective are presented in the “Complementary Controls at User Entities” within Section 3.
Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that CenturyLink’s data centers, system and network equipment, and storage media are protected from unauthorized access.

<table>
<thead>
<tr>
<th>#</th>
<th>Control Activity Specified by the Service Organization</th>
<th>Test Applied by the Service Auditor</th>
<th>Test Results</th>
</tr>
</thead>
</table>
| 1.01 | Physical security policies and procedures are in place to guide personnel in the following areas:  
• Data center access for employees, contractors and visitors  
• Security monitoring  
• Security assessments and access activity reviews | Inspected the physical security policies and procedures to determine that physical security policies and procedures were in place to guide personnel in the following areas:  
• Data center access for employees, contractors and visitors  
• Security monitoring  
• Security assessments and access activity reviews | No exceptions noted. |
| 1.02 | Site authorizers are utilized to approve permanent access to the data centers. | Inquired of the global data center physical security manager regarding data center access to determine that site authorizers were utilized to approve access requests for individuals who required permanent access to the data centers.  
Inspected the data center site authorizer listing for each data center to determine that a defined set of site authorizers was utilized to approve permanent access to the data centers. | No exceptions noted. |
| 1.03 | Security access controls (i.e. physical barriers and doors, card controlled entry points, biometric scanning, video surveillance and/or manned reception desks) are utilized to protect areas that contain information and information processing facilities. | Inquired of the data center personnel regarding data center security to determine that security access controls were utilized to protect areas that contained information processing facilities.  
Observed the security access controls at each data center to determine that security access controls were utilized to protect areas that contained information and information processing facilities. | No exceptions noted. |
<table>
<thead>
<tr>
<th>#</th>
<th>Control Activity Specified by the Service Organization</th>
<th>Test Applied by the Service Auditor</th>
<th>Test Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.04</td>
<td>Control mechanisms are in place to limit physical access to restricted data center areas such as the raised floor, equipment rooms, transport areas, and critical power and mechanical infrastructure.</td>
<td>Inquired of the data center personnel regarding data center security to determine that control mechanisms were in place to limit physical access to restricted data center areas such as the raised floor, equipment rooms, transport areas, and critical power and mechanical infrastructure.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td></td>
<td>Observed the facility entrances and interior access points at each data center to determine that control mechanisms were in place to limit physical access to the raised floor, equipment room, transport areas, and critical power and mechanical infrastructure.</td>
<td></td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td>1.05</td>
<td>Data center badge access requests for CenturyLink employees and contractors require a completed badge access request approved by site authorizers. Badge access requests for customers require a completed badge access request approved by an authorized customer representative.</td>
<td>Inquired of the data center personnel regarding data center access to determine that data center badge access requests for employees and contractors required a completed badge access request approved by site authorizers, and badge access requests for customers required a completed badge access request approved by an authorized customer representative.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td></td>
<td>Inspected the badge access requests for a sample of employees, contractors and customers granted permanent access to a sample of data centers during the review period to determine that badge access requests were approved by site authorizers or customer representatives, as applicable, for each employee, contractor, customer and data center sampled.</td>
<td></td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td>#</td>
<td>Control Activity Specified by the Service Organization</td>
<td>Test Applied by the Service Auditor</td>
<td>Test Results</td>
</tr>
<tr>
<td>----</td>
<td>-------------------------------------------------------</td>
<td>-------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>1.06</td>
<td>Data center security personnel undergo an annual certification process to maintain awareness and help ensure adherence to current physical security policies and procedures.</td>
<td>Inquired of the physical security manager regarding security training to determine that data center security personnel underwent an annual certification process to maintain awareness and help ensure adherence to current physical security policies and procedures.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Inspected the annual certification training results for a sample of current data center security operations personnel to determine that each employee sampled completed the annual certification training during the review period.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td>1.07</td>
<td>Data center access for CenturyLink personnel is revoked as a component of the employee termination process.</td>
<td>Inspected the data center badge access permissions for a sample of employees terminated during the review period to determine that data center access was revoked for each CenturyLink terminated employee sampled.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td>1.08</td>
<td>Temporary access to the data centers for CenturyLink contractors must be pre-approved by work order or ticket. Temporary access to data centers for customers require prior authorization by the authorized customer representative.</td>
<td>Inquired of the physical security manager regarding temporary data center access to determine that temporary access to the data centers for CenturyLink contractors required pre-approval by work order or ticket, and temporary access to data centers for customers required prior authorization by the authorized customer representative.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Inspected the access request documentation for example vendors and contractors granted temporary access to a sample of data centers during the review period to determine that access was pre-approved by work order, ticket, or customer authorization for each vendor, contractor and data center sampled.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td>#</td>
<td>Control Activity Specified by the Service Organization</td>
<td>Test Applied by the Service Auditor</td>
<td>Test Results</td>
</tr>
<tr>
<td>-----</td>
<td>--------------------------------------------------------</td>
<td>-------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td></td>
<td>Inspected the customer badge access listings maintained within the OpStats Portal to determine that customer-maintained access lists were utilized to identify customer representatives authorized for temporary access to the data centers.</td>
<td>No exceptions noted.</td>
<td></td>
</tr>
<tr>
<td>1.09</td>
<td>Customer-maintained access lists are utilized to identify customer representatives authorized to request permanent or temporary access to the data center(s) where the customer colocation space resides.</td>
<td>Inquired of the data center personnel regarding customer access to determine that customer-maintained access lists were utilized to identify customer representatives authorized to request permanent or temporary access to the data center(s) where the customer colocation space resided.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td></td>
<td>Inspected the customer badge access listings maintained within the OpStats Portal to determine that customer-maintained access lists were utilized to identify customer representatives authorized to request permanent or temporary access to the data center(s) where the customer colocation space resided.</td>
<td>No exceptions noted.</td>
<td></td>
</tr>
<tr>
<td>1.10</td>
<td>Visitor logs are maintained for at least 90 days to document visitor activity at the data centers.</td>
<td>Inspected the visitor log for each data center for a sample of dates during the review period to determine that a visitor log was maintained for at least 90 days at each data center.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td>1.11</td>
<td>Visitors are required to be escorted by an authorized CenturyLink employee or authorized customer representative at all times while in the data centers.</td>
<td>Inquired of the data center personnel regarding visitor access to determine that visitors were required to be escorted by a CenturyLink employee or authorized customer representative at all times while in the data centers.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td></td>
<td>Observed the visitor access procedures at each data center to determine that visitors were escorted by a CenturyLink employee or authorized customer representative while in the data centers.</td>
<td>No exceptions noted.</td>
<td></td>
</tr>
<tr>
<td>#</td>
<td>Control Activity Specified by the Service Organization</td>
<td>Test Applied by the Service Auditor</td>
<td>Test Results</td>
</tr>
<tr>
<td>-----</td>
<td>-------------------------------------------------------</td>
<td>-------------------------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>1.12</td>
<td>All persons entering the data centers must present valid government-issued photo ID, or display and use a valid CenturyLink photo access badge prior to entering the facility.</td>
<td>Inquired of the data center personnel regarding data center access procedures to determine that persons entering the data centers were required to provide valid government-issued photo ID, or display and use a valid CenturyLink photo access badge prior to entering the facility.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td></td>
<td>Observed the access procedures at each data center to determine that persons entering the data centers were required to provide valid government-issued photo ID, or display and use a valid CenturyLink photo access badge prior to entering the facility.</td>
<td></td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td>1.13</td>
<td>CCTV surveillance video and/or ACS activity logs are retained for a minimum of 90 calendar days.</td>
<td>Inquired of the data center personnel regarding data center monitoring to determine that CCTV surveillance video and/or ACS activity logs were retained for a minimum of 90 calendar days.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td></td>
<td>Inspected captured screen images from the CCTV surveillance system and/or activity logs from the ACS for each data center to determine that CCTV surveillance video and/or ACS activity logs were retained for a minimum of 90 calendar days.</td>
<td></td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td>1.14</td>
<td>Data center security personnel and the CSOC monitor access to the data centers 24 hours a day, seven days a week, using reports from the physical security access mechanisms, alarms and CCTV video surveillance systems.</td>
<td>Inquired of the data center personnel regarding data center security to determine that data center security personnel and the CSOC monitored access to the data centers 24 hours a day, seven days a week, using reports from the physical security access mechanisms, alarms and CCTV video surveillance systems.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td>#</td>
<td>Control Activity Specified by the Service Organization</td>
<td>Test Applied by the Service Auditor</td>
<td>Test Results</td>
</tr>
<tr>
<td>----</td>
<td>------------------------------------------------------</td>
<td>-------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>Observed a sample of devices and monitoring reports generated during the review period to determine that data center security personnel and the CSOC monitored access to the data centers using reports from the physical security access mechanisms, alarms and CCTV video surveillance systems.</td>
<td>No exceptions noted.</td>
<td></td>
</tr>
<tr>
<td>1.15</td>
<td>Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises are controlled and, where applicable, are isolated from information processing facilities to avoid unauthorized access.</td>
<td>Inquired of the data center personnel regarding data center security to determine that access points such as delivery and loading areas and other points where unauthorized persons could enter the premises were controlled and, where applicable, were isolated from information processing facilities to avoid unauthorized access.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td></td>
<td>Observed the data centers to determine that access points such as delivery and loading areas and other points where unauthorized persons could enter the premises were controlled and, where applicable, were isolated from information processing facilities to avoid unauthorized access.</td>
<td>No exceptions noted.</td>
<td></td>
</tr>
<tr>
<td>1.16</td>
<td>An inventory of access badges and metal keys designated for loan to employees, customers, or contractors, as applicable by location, is performed at least once per day to account for all badges and metal keys.</td>
<td>Inquired of the data center personnel regarding data center security to determine that an inventory of access badges and metal keys designated for loan to employees, customers, or contractors, as applicable by location, was performed at least once per day to account for all badges and metal keys.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td></td>
<td>Inspected the completed inventory of access badges and metal keys designated for loan to employees, customers, or contractors for a sample of dates and facilities to determine that an inventory was performed at least once per day for each date and data center facility sampled.</td>
<td>No exceptions noted.</td>
<td></td>
</tr>
<tr>
<td>#</td>
<td>Control Activity Specified by the Service Organization</td>
<td>Test Applied by the Service Auditor</td>
<td>Test Results</td>
</tr>
<tr>
<td>-----</td>
<td>-------------------------------------------------------</td>
<td>-----------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>1.17</td>
<td>All shipments received at the data centers are stored in a physically secured location.</td>
<td>Inquired of the data center personnel regarding data center security to determine that shipments received at the data centers were stored in a physically secured location.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Observed the shipping and receiving procedures at each data center to determine that shipments received at the data centers were stored in a physically secured location.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td>1.18</td>
<td>Access to the shipping and receiving areas at the data centers is restricted to authorized personnel.</td>
<td>Inquired of the data center personnel regarding data center security to determine that access to the shipping and receiving areas at the data centers was restricted to authorized personnel.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Observed the shipping and receiving areas at each data center to determine that access to the shipping and receiving areas at the data centers was restricted.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td>1.19</td>
<td>The compliance program management team risk ranks each data center and performs reviews of the data centers based on risk ranking on an annual basis to help ensure physical and environmental security policies and procedures are followed. Findings of noncompliance are reported to data center security personnel or facility management personnel for remediation.</td>
<td>Inquired of the senior information security auditor regarding the data center review process to determine that the compliance program management team risk ranked each data center and reviewed the data centers based on risk ranking on an annual basis to help ensure physical and environmental security policies and procedures were followed and findings of noncompliance were reported to data center security personnel or facility management personnel for remediation.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td>#</td>
<td>Control Activity Specified by the Service Organization</td>
<td>Test Applied by the Service Auditor</td>
<td>Test Results</td>
</tr>
<tr>
<td>----</td>
<td>------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Inspected the most recent data center risk ranking / site visit schedule and the feedback forms for each data center</td>
<td></td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td></td>
<td>scheduled to undergo a site visit during the review period to determine that the compliance program management team</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>assessed risk for each data center, prepared a site visit schedule, and performed a review of each data center scheduled</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>to undergo a site visit during the review period.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### ENVIRONMENTAL SECURITY

**Control Objective Specified by the Service Organization:** Control activities provide reasonable assurance that CenturyLink facilities housing customer equipment and support operations are protected from certain environmental threats (power loss, fire, temperature and humidity levels).

<table>
<thead>
<tr>
<th>#</th>
<th>Control Activity Specified by the Service Organization</th>
<th>Test Applied by the Service Auditor</th>
<th>Test Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.01</td>
<td>Environmental security policies and procedures are in place to guide personnel in the following areas:</td>
<td>Inspected the environmental security policies and procedures document to determine that environmental security policies and procedures were in place to guide personnel in the following areas:</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td></td>
<td>• Equipment specifications and operating instructions</td>
<td>• Equipment specifications and operating instructions</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Equipment inspections</td>
<td>• Equipment inspections</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Preventive maintenance schedules (internal and external maintenance activities)</td>
<td>• Preventive maintenance schedules (internal and external maintenance activities)</td>
<td></td>
</tr>
<tr>
<td>2.02</td>
<td>A BMS is configured to monitor data center equipment including, but not limited to, the following:</td>
<td>Observed the BMS at each data center to determine that a BMS was configured to monitor applicable data center equipment that included the following:</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td></td>
<td>• Fire detection and suppression systems, as applicable</td>
<td>• Fire detection and suppression systems</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• HVAC units</td>
<td>• HVAC units</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Generators, as applicable</td>
<td>• Generators</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Electrical systems, as applicable</td>
<td>• Electrical systems</td>
<td></td>
</tr>
<tr>
<td>#</td>
<td>Control Activity Specified by the Service Organization</td>
<td>Test Applied by the Service Auditor</td>
<td>Test Results</td>
</tr>
<tr>
<td>-----</td>
<td>-------------------------------------------------------</td>
<td>------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>2.03</td>
<td>The BMS is configured to notify data center staff either via on-screen alert or e-mail alert when predefined thresholds are exceeded on monitored devices.</td>
<td>Inquired of the data center personnel regarding BMS alerts to determine that the BMS was configured to notify data center staff either via on-screen alert or e-mail alert when predefined thresholds were exceeded on monitored devices.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Inspected captured screen images of on-screen alerts from the BMS for a sample of data centers to determine that the BMS was configured to notify data center staff via on-screen alert when predefined thresholds were exceeded on monitored devices.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Inspected the BMS notification configurations and example alerts generated during the review period for a sample of data centers to determine that the BMS was configured to notify data center staff via e-mail alert when predefined thresholds were exceeded on monitored devices.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td>2.04</td>
<td>Power management equipment is in place at each data center.</td>
<td>Observed the power management equipment at each data center to determine that power management equipment was in place.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td>2.05</td>
<td>Third party specialists inspect power management systems according to a predefined maintenance schedule.</td>
<td>Inquired of the data center personnel regarding power management systems to determine that third party specialists inspected the power management systems at each data center on an annual basis.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Inspected the most recent power management systems inspection reports for a sample of data centers to determine that third party specialists inspected the power management systems on an annual basis.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td>2.06</td>
<td>Fire detection and suppression equipment is in place at each data center.</td>
<td>Observed the fire detection and suppression equipment at each data center to determine that fire detection and suppression equipment was in place.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td>#</td>
<td>Control Activity Specified by the Service Organization</td>
<td>Test Applied by the Service Auditor</td>
<td>Test Results</td>
</tr>
<tr>
<td>-----</td>
<td>--------------------------------------------------------</td>
<td>-------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>2.07</td>
<td>Third party specialists inspect fire detection and suppression systems on an annual basis.</td>
<td>Inquired of the data center personnel regarding fire detection and suppression equipment to determine that third party specialists inspected the fire detection and suppression equipment on an annual basis.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Inspected the most recent fire detection and suppression equipment inspection reports for a sample of data centers to determine that third party specialists inspected the fire detection and suppression equipment on an annual basis.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td>2.08</td>
<td>HVAC systems are in place at each data center.</td>
<td>Observed the HVAC systems at each data center to determine that HVAC systems were in place.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td>2.09</td>
<td>Third party specialists inspect HVAC systems and water detection sensors, as applicable, on an annual basis.</td>
<td>Inquired of the data center personnel regarding HVAC systems and water detection sensors to determine that third party specialists inspected the HVAC systems and water detection sensors, as applicable, at each data center on an annual basis.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Inspected the most recent HVAC systems and water detection sensors inspection reports for a sample of data centers to determine that third party specialists inspected the HVAC systems and water detection sensors, as applicable, on an annual basis.</td>
<td>No exceptions noted.</td>
</tr>
</tbody>
</table>
2.10 The compliance program management team risk ranks each data center and performs reviews of the data centers based on risk ranking on an annual basis to help ensure physical and environmental security policies and procedures are followed. Findings of noncompliance are reported to data center security personnel or facility management personnel for remediation.

Inquired of the senior information security auditor regarding the data center review process to determine that the compliance program management team risk ranked each data center and reviewed the data centers based on risk ranking on an annual basis to help ensure physical and environmental security policies and procedures were followed and findings of noncompliance were reported to data center security personnel or facility management personnel for remediation.

Inspected the most recent data center risk ranking / site visit schedule and the feedback forms for each data center scheduled to undergo a site visit during the review period to determine that the compliance program management team assessed risk for each data center, prepared a site visit schedule, and performed a review of each data center scheduled to undergo a site visit during the review period.

No exceptions noted.

### MEDIA HANDLING

**Control Objective Specified by the Service Organization:** Control activities provide reasonable assurance that CenturyLink and customer backup media is secured, tracked and access to backup media is limited to authorized individuals.

<table>
<thead>
<tr>
<th>#</th>
<th>Control Activity Specified by the Service Organization</th>
<th>Test Applied by the Service Auditor</th>
<th>Test Results</th>
</tr>
</thead>
</table>
| 3.01 | Documented procedures are in place to guide personnel in media handling procedures that include, but are not limited to, the following:  
• Tape ejection steps  
• Tape storage procedures  
• Tape tracking | Inspected the media handling procedures to determine that documented procedures were in place to guide personnel in media handling procedures that included the following:  
• Tape ejection steps  
• Tape storage procedures  
• Tape tracking | No exceptions noted. |
<table>
<thead>
<tr>
<th>#</th>
<th>Control Activity Specified by the Service Organization</th>
<th>Test Applied by the Service Auditor</th>
<th>Test Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.02</td>
<td>The backup libraries are secured in locked and restricted areas at the data center locations.</td>
<td>Observed the backup libraries during the review period for a sample of data center facilities to determine that the backup libraries were secured in locked cages at each data center sampled.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td>3.03</td>
<td>A third party media storage provider is utilized to provide secure transport and storage of backup media.</td>
<td>Inquired of data center personnel regarding the rotation of backup media to determine that a third party media storage provider was utilized to provide secure transport and storage of backup media.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Inspected the media handling reports for a sample of data center facilities during the review period to determine that a third party media storage provider was utilized to provide secure transport and storage of backup media for each data center sampled.</td>
<td>No exceptions noted.</td>
</tr>
</tbody>
</table>
| 3.04 | Off-site backup media are tracked in a tracking system that lists details including, but not limited to, the following:  
• Date received  
• Date sent off-site | Inspected the media handling reports for a sample of months during the review period to determine that off-site backup media were recorded in a tracking system that included the following details:  
• Date received  
• Date sent off-site | No exceptions noted. |
| 3.05 | Containers holding backup media to be taken off-site by the third party media storage provider are secured in a locked case and/or a restricted area of the data center. | Observed backup media awaiting transport at a sample of data center facilities during the review period to determine that containers holding backup media to be taken off-site by the third party media storage provider were secured in a locked case and/or a restricted area of each data center sampled. | No exceptions noted. |
SECTION 5

OTHER INFORMATION PROVIDED BY MANAGEMENT
CONTINGENCY AND RECOVERY STATEMENT FOR CUSTOMERS

CenturyLink Contingency and Recovery Guidelines

In today’s global information age, CenturyLink recognizes that unexpected situations may occur that can impact an organization’s operations and limit its ability to deliver services to end users (e.g., customers, field offices, governmental agencies, and the public).

CenturyLink has predetermined and pre-established recovery strategies to maintain a resilient continuity state for its own vital infrastructure to provide for the swift and seamless recovery of CenturyLink systems, with minimal disruption to its own internal operations.

CenturyLink management is committed to maintaining resilience of critical infrastructure by conducting periodic testing as jointly directed by CenturyLink’s corporate information security, engineering, and compliance management departments. Recovery strategies receive ongoing reviews to evaluate current and future risk in order to maintain appropriate procedures and responses.

Contingency Guidelines

CenturyLink has implemented a straightforward strategic approach toward recovery. Strategies are designed to handle ‘high impact,’ unforeseen business disruptions varying in length and scope, where each CenturyLink facility is capable of recovering CenturyLink-identified functions according to their critical timeliness.

The CenturyLink strategy is comprised of the following components:

- Identification of CenturyLink’s mission critical systems, related recovery objectives, and backup systems
- Review of CenturyLink financial and operational risk
- Employee safety and communications
- Alternate recovery site and preparedness for CenturyLink critical systems
- Manned and electronic security management and managed network security verification at all CenturyLink facilities
- Customer notification preparedness through predetermined event management protocols
- Insurance for critical equipment

The CenturyLink strategy is consistent with well-defined industry-standard contingency planning methods and practices, along with dedicated continuity planners who manage planning and evaluation of CenturyLink’s contingency strategy.

Contingency Statement and Recovery

As the building blocks toward mitigating the reduction of risk and the impact of a potential outage, the CenturyLink strategy is designed to restore operability of its targeted systems, applications, and facilities in the event of an outage or emergency with the following elements in conjunction with the above items:

- Resilient Network Infrastructure – The main goal is to withstand any single physical fault that occurs on CenturyLink long-haul circuits (intercity trunks), short hauls (connecting points of presence (PoPs) within a city), central processor cards, input/output processor cards, fans, power supplies, power grids, and HVAC. The CenturyLink network is built with particular attention to redundancy, diversity, and fault tolerance for CenturyLink’s critical systems and infrastructures.

- Hardened Data Center Facilities – CenturyLink operates 55 manned and electronically secured data centers located in the US, Europe the Middle East and Africa (EMEA), and Asia. Each data center maintains specific protocols for emergency and disastrous situations and conditions. Mandatory
structural (in California this also includes seismic bracing), mechanical, utility, and fire/life/safety systems are in place to provide adequate levels of security and recovery.

- Notification to Customers – Notification procedures have been predetermined to address conditions surrounding an outage that may impact various services. CenturyLink maintains decentralized and geographically deployed SSCs to handle communications both internally and externally in order to maintain the highest level of quality and SSC availability.

Each of these integrated processes reinforces the essential organizational framework safeguarding against natural, technological, and human-error events. Key management and technical personnel are also available 24x7 to service and maintain CenturyLink’s critical systems and functionality.

Customer Obligations

As the CenturyLink contingency strategy addresses points of failure within the CenturyLink organizational infrastructure and the deployment of recovery processes to provide business stability, the customer may also benefit indirectly as a result of CenturyLink’s recovery strategy. However, it remains the customer’s responsibility for developing, implementing, identifying, and maintaining their own business continuity or disaster recovery (BC/DR) policies and planning as required by their organization or regulatory requirements. CenturyLink’s contingency strategies are solely intended for its own internal infrastructure and are not intended to replace any customer-specific BC/DR plan or satisfy any BC/DR planning requirements. CenturyLink cannot state nor guarantee that: (a) CenturyLink’s contingency and recovery strategy will adequately address all disasters or emergencies, including regional blackouts, natural disasters, pandemic disease outbreaks, terrorist attacks or other crises of a local, national or international scope, or (b) that the CenturyLink data centers or the services it provides will not be impacted by such disaster or emergency conditions. While CenturyLink’s contingency and recovery strategy is not intended as a surrogate for its customers’ own business recovery and continuity planning, customers may engage CenturyLink professional services consultants to design and implement contingency programs if they desire. Services are subject to terms, conditions, and charges set forth in applicable CenturyLink service agreements and statement of work.

CenturyLink Advisory

With respect to pandemic disease outbreaks, CenturyLink will contact the World Health Organization (WHO) and Center for Disease Control (CDC) and follow their guidance on how to prepare and/or address situations as they may arise.

CenturyLink’s preparedness may include putting contingency plans in place to address issues, including coordinating the CenturyLink emergency response teams for all affected sites, and monitoring the situation in order to make changes as the situation warrants. All CenturyLink regions, including US, EMEA, and Asia Pacific (APAC), will follow these guidelines and will work with their local leadership to take any precautions necessary to address customer support requirements, governmental restrictions and local conditions.

Disclaimer

This contingency and recovery strategy statement is for informational purposes only and is subject to change from time to time in CenturyLink’s sole discretion and without notice. As it is solely the responsibility of the customer to develop, identify and maintain its own BC/DR policies and planning for all purposes, this statement is not intended, nor shall it be incorporated or referred to any contract or agreement between CenturyLink and customer. CenturyLink does not disclose the specific details of its contingency and recovery strategy plans to customers or other third parties, as they are considered highly proprietary information and held in strict confidence.

CenturyLink cannot, and does not state nor guarantee that CenturyLink’s contingency and recovery strategy will adequately address all disasters or emergencies, including regional blackouts, natural disasters, pandemic disease outbreaks, terrorist attacks or other crises of a local, national or international scope, or that the CenturyLink data centers or CenturyLink services will not be impacted by such disaster or emergency conditions.