System and Organization Controls 2 Type II Report

ViaWest, Inc.'s Description of Its Colocation, Managed Services, and Client Center Cloud System

for the Period October 1, 2016 to September 30, 2017

With Independent Service Auditor's Report,
Including Tests Performed and Results Thereof

ViaWest, Inc.

Colocation, Managed Services, and Client Center Cloud System

TABLE OF CONTENTS

SECTION I. ASSERTION OF VIAWEST, INC.

Assertion of ViaWest, Inc.

December 6, 2017

We have prepared the accompanying *ViaWest, Inc.'s Description of Its Colocation, Managed Services, and Client Center Cloud System for the Period October 1, 2016 to September 30, 2017* (Description) of ViaWest, Inc. (ViaWest or Service Organization) based on the criteria in items (a)(i)-(ii) below, which are the criteria for a description of a service organization's system in paragraph 1.26 of the American Institute of Certified Public Accountants (AICPA) Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy (SOC 2®)* (Description Criteria). The Description is intended to provide users with information about the ViaWest Colocation, Managed Services, and Client Center Cloud System (System) that may be useful when assessing the risks from interactions with the System throughout the period October 1, 2016 to September 30, 2017, particularly information about the suitability of design and operating effectiveness of ViaWest's controls to meet the criteria related to security and availability set forth in TSP section 100 A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services criteria).

ViaWest uses 2001 Sixth, LLC dba Westin Building Exchange (Westin) and Equinix, Inc. (Equinix) to provide physical access and environmental controls for certain locations within the Client Center Cloud environment. The Description includes only the controls of ViaWest and excludes controls of the subservice organizations. The Description also indicates that certain trust services criteria specified therein can be met only if Westin and Equinix's controls assumed in the design of ViaWest's controls are suitably designed and operating effectively along with the related controls at the Service Organization. The Description does not extend to controls of Westin or Equinix.

The Description also indicates that certain trust services criteria specified in the Description can be met only if complementary user entity controls assumed in the design of ViaWest's controls are suitably designed and operating effectively, along with related controls at the Service Organization. The Description does not extend to controls of user entities.

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

a. the Description fairly presents the System throughout the period October 1, 2016 to September 30, 2017, based on the following description criteria:

i. the Description contains the following information:

(1) The types of services provided.

(2) The components of the System used to provide the services, which are the following:

- Infrastructure. The physical structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and other telecommunications networks).
- Software. The application programs and IT system software that support application programs (operating systems, middleware, and utilities).[1]
- People. The personnel involved in the governance, operation and use of a system (developers, operators, entity users, vendor personnel, and managers).
- Procedures. The automated and manual procedures.[2]
- Data. Transaction streams, files, databases, tables, and output used or processed by the system). [3]

(3) The boundaries or aspects of the System covered by the Description.

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

- How such information is provided or received and the role of the subservice organization or other parties.
- The procedures the service organization performs to determine that such information and its processing, maintenance, and storage are subject to appropriate controls.

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

- Complementary user-entity controls contemplated in the design of the service organization's system.
- When the inclusive method is used to present a subservice organization, controls at the subservice organization.

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

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

[1] The focus of this report is the ViaWest, Inc. Colocation System, Managed Services, and Client Center Cloud only. In this system, ViaWest, Inc. does not provide application services for its customers. Accordingly, our Description does not address certain items in criterion (a)(i)(2).

[2] The description of the procedures of the system includes those by which services are provided, including, as appropriate, procedures by which service activities are initiated, authorized, performed, delivered, and reports and other information prepared.

[3] The focus of this report is the ViaWest, Inc. Colocation System, Managed Services, and Client Center Cloud only. In this system, ViaWest, Inc. does not process customer data. Accordingly, our Description does not address certain items in criterion (a)(i)(2).

(7) Any applicable trust services criteria that are not addressed by a control at the service organization or a subservice organization and the reasons.

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

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

b. The controls stated in the Description were suitably designed to provide reasonable assurance that the applicable trust services criteria were met, if the controls operated as described and if user entities applied the complementary user entity controls and the subservice organizations applied the controls assumed in the design of ViaWest, Inc.'s controls throughout the period October 1, 2016 to September 30, 2017.

c. The ViaWest controls stated in the description operated effectively throughout the period October 1, 2016 to September 30, 2017 to meet the applicable trust services criteria if user entities applied the complementary user entity controls and the subservice organizations applied the controls assumed in the design of ViaWest's controls throughout the period October 1, 2016 to September 30, 2017.

ViaWest, Inc.

SECTION II. INDEPENDENT SERVICE AUDITOR'S REPORT

Ernst & Young LLP
Suite 3300
370 17th Street
Denver, CO 80202

Tel: +1 720 931 4000
Fax: +1 720 931 4444
ey.com

Independent Service Auditor's Report

The Board of Directors
ViaWest, Inc.

Scope

We have examined ViaWest, Inc.'s accompanying *ViaWest, Inc.'s Description of Its Colocation, Managed Services, and Client Center Cloud System for the Period October 1, 2016 to September 30, 2017* (Description) based on the criteria set forth in paragraph 1.26 of the American Institute of Certified Public Accountants (AICPA) Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy (SOC 2®)* (description criteria) and the suitability of the design and operating effectiveness of controls included in the Description throughout the period October 1, 2016 to September 30, 2017 to meet the criteria for security and availability set forth in TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services criteria).

ViaWest uses 2001 Sixth, LLC dba Westin Building Exchange (Westin) and Equinix, Inc. (Equinix) to provide physical access and environmental controls for certain locations within the Client Center Cloud environment. The Description indicates that certain applicable trust services criteria can be met only if Westin and Equinix's controls, assumed in the design of ViaWest's controls, are suitably designed and operating effectively along with related controls at the service organization. The description presents ViaWest's system; its controls relevant to the applicable trust services criteria; and the types of controls that the service organization assumes have been implemented, suitably designed, and operating effectively at Westin and Equinix. Our examination did not extend to the services provided by Westin and Equinix and we have not evaluated whether the controls management assumes have been implemented at Westin and Equinix have been implemented or whether such controls were suitably designed and operating effectively throughout the period October 1, 2017 to September 30, 2017.

The Description also indicates that certain applicable trust services criteria can be met only if complementary user entity controls assumed in the design of ViaWest's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

ViaWest's responsibilities

ViaWest has provided the accompanying assertion titled, *Assertion of ViaWest, Inc.* (Assertion), about the fairness of the presentation of the Description based on the description criteria and suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria. ViaWest is responsible for (1) preparing the Description and Assertion; (2) the completeness, accuracy, and method of presentation of the Description and

Assertion; (3) providing the services covered by the Description; (4) identifying the risks that would prevent the applicable trust services criteria from being met; and (5) designing, implementing, and documenting controls that are suitably designed and operating effectively to meet the applicable trust services criteria 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 described therein to meet the applicable trust services criteria, based on our examination.

Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the Description is fairly presented based on the description criteria, and (2) the controls described therein are suitably designed and operating effectively to meet the applicable trust services criteria throughout the period October 1, 2016 to September 30, 2017. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- Performing procedures to obtain evidence about the fairness of the presentation of the Description based on the description criteria and the suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria.
- Assessing the risks that the Description is not fairly presented and that the controls were not suitably designed or operating effectively to meet the applicable trust services criteria.
- Testing the operating effectiveness of those controls to provide reasonable assurance that the applicable trust services criteria were met.
- Evaluating the overall presentation of the Description.

Inherent limitations

The Description is prepared to meet the common needs of a broad range of users, and may not, therefore, include every aspect of the system that each individual user may consider important to its own particular needs. Because of their nature, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. Also, the projection to the future of any evaluation of the fairness of the presentation of the Description, or conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable trust services criteria is subject to the risk that the system may change or that controls at a service organization may become ineffective.

Building a better working world

Description of tests of controls

The specific controls we tested and the nature, timing, and results of those tests are listed in the accompanying *Description of Criteria, Controls, Tests, and Results of Tests* section (Description of Tests and Results).

Opinion

In our opinion, in all material respects, based on the description criteria and the applicable trust services criteria:

a. The Description fairly presents the ViaWest Colocation, Managed Services, and Client Center Cloud System that was designed and implemented throughout the period October 1, 2016 to September 30, 2017.

b. The controls stated in the Description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively and if the subservice organizations and user entities applied the controls assumed in the design of ViaWest's controls throughout the period October 1, 2016 to September 30, 2017.

c. The controls operated effectively to provide reasonable assurance that the applicable trust services criteria were met throughout the period October 1, 2016 to September 30, 2017, if the subservice organizations and user entity controls assumed in the design of ViaWest Inc.'s controls operated effectively throughout the period October 1, 2016 to September 30, 2017.

Restricted use

This report, including the description of tests of controls and results thereof in the Description of Tests and Results, is intended solely for the information and use of ViaWest Inc., user entities of ViaWest Inc.'s Colocation, Managed Services, and Client Center Cloud System during some or all of the period October 1, 2016 to September 30, 2017 and prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, subservice organizations, or other parties including complementary user entity controls and subservice organization controls assumed in the design of the service organization's controls
- Internal control and its limitations

- User entity responsibilities and how they interact with related controls at the service organization
- The applicable trust services criteria
- The risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks

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

Ernst & Young LLP

December 6, 2017

SECTION III. DESCRIPTION OF VIAWEST, INC.'S COLOCATION, MANAGED SERVICES, AND CLIENT CENTER CLOUD SYSTEM FOR THE PERIOD OCTOBER 1, 2016 TO SEPTEMBER 30, 2017

1 Scope of This Report

This report includes a description of ViaWest's Colocation, Managed Services, and Client Center System provided at data centers located in Denver, Colorado; Salt Lake City, Utah; Hillsboro, Oregon; Las Vegas, Nevada; Austin, Texas; Dallas, Texas; Phoenix, Arizona; Minneapolis, Minnesota; Allentown, Pennsylvania; and Calgary, Alberta (Canada) that may be relevant to the internal control of user entities (also referred to as customers or customer organizations). This report is focused solely on Colocation services, Managed Services, and the Client Center Cloud and does not extend to managed or cloud services, such as the Compliant Cloud Environment.

The following description is intended to provide ViaWest customer organizations and the independent auditors of those customer organizations with information about the control activities of the services provided by ViaWest. The description of the System includes certain information technology (IT) general controls that support the delivery of ViaWest's services. This report does not encompass all aspects of the services provided or procedures followed in connection with the System.

The following description is intended to provide sufficient information for such user entities to obtain an understanding of the System and controls in place over ViaWest's services. The description has been prepared in accordance with the guidance contained in the American Institute of Certified Public Accountants' (AICPA) TSP Section 100A, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, including its respective amendments and interpretations.

2 Overview of ViaWest

ViaWest was founded in 1999, and is headquartered in Denver, Colorado. During its 18-year history, ViaWest has grown both organically and through acquisition currently employs over 500 employees across the United States. ViaWest was acquired by Peak 10, Inc. (Peak 10), headquartered in Charlotte, North Carolina, in August 2017 and is now a wholly owned subsidiary of Peak 10.

3 Overview of ViaWest's Colocation, Managed Services, and Client Center Cloud

ViaWest offers a variety of customized products from strictly colocation through fully managed cloud environments. Colocation services are limited to power, environmental, physical security, and network connectivity services. Managed Services can include ViaWest support for a variety of systems, and can include the hardware, spare parts, day-to-day operating system and database maintenance and support, patching, updates, configuration management, security, and monitoring. The Client Center Cloud provides infrastructure as a service offering for either private or public cloud environments. ViaWest's services related to the private or public cloud solutions other than the Client Center Cloud are not included in the scope of this report.

ViaWest provides services in nine geographic locations within the United States and one within Canada. With 30 physical data center locations and growing, ViaWest operates raised floor gross square footage of more than 800,000 square feet. ViaWest's data center facilities are currently provided from the following regional locations:

- Denver, Colorado
- Salt Lake City, Utah
- Las Vegas, Nevada
- Hillsboro, Oregon
- Austin, Texas
- Dallas, Texas
- Phoenix, Arizona
- Minneapolis, Minnesota
- Allentown, Pennsylvania
- Calgary, Alberta (Canada)

The in-scope ViaWest Managed Services are physically hosted at the Cornell (Denver, Colorado), Arapahoe (Denver, Colorado), Delong (Salt Lake City, Utah), and Synergy Park (Dallas, Texas) locations. Additionally, some network-managed services are available at all ViaWest locations. The Client Center Cloud is physically hosted in the Allentown, Pennsylvania; Compark (Denver, Colorado); and Brookwood (Hillsboro, Oregon) data centers in addition to the following sub-service provider locations:

Subservice Provider	Location
Equinix	Amsterdam, Netherlands
Equinix	Ashburn, Virginia
Equinix	London, United Kingdom
Westin	Seattle, Washington

Controls at the subservice organizations are not included within the scope of this report.

ViaWest services are supported by a number of functional groups, each with its own roles and responsibilities specific to supporting the business. Management responsibilities within ViaWest have been segregated by appropriate functions, with vice presidents, directors, and managers providing leadership and accountability for their respective areas.

The ViaWest team works closely with clients to understand their business needs, and acts as an extension of their IT team, with assigned engineering and operations resources performing daily operational support for their environments. These environments are monitored and supported 24x7 by the local Data Center Customer Support (DCCS) or remote ViaWest Technical Assistance Center (VTAC) support team. ViaWest leverages formal processes of requirements definition, provisioning, change management, incident management, and monitoring to manage these customer environments.

All data center operations are supported and managed by the Cadence and Cerberus ticketing systems. The systems are used to notify, track, and manage any issues that may arise within the data centers. Logical access to various systems is controlled via Windows Active Directory or through access control lists (ACLs) defined on network devices. ViaWest also uses security measures to help ensure that access to network devices is controlled in a secure manner using encryption and strong password and security settings.

ViaWest's data center facilities are equipped with the latest environmental and security equipment, including redundant heating, ventilation and air conditioning (HVAC) systems; dry pipe and multi-zone fire detection systems; uninterruptible power supply (UPS); and generator backups for all data center operations. ViaWest has also implemented physical access measures such as badge card access, personal identification numbers (PINs) and biometric fingerprint scans, and video surveillance with 24-hour monitoring by the DCCS and VTAC.

4 Relevant Aspects of the Control Environment, Risk Management, Information and Communication, Control Activities and Monitoring

Control Environment

Integrity and Ethical Values

Integrity and high ethical standards are qualities essential to the business of ViaWest and are fundamental standards of behavior for employees. At ViaWest, the standards of integrity and ethics are demonstrated daily by the personal conduct of management and various controls, including guidelines for handling sensitive information, invention agreements, security policies, and policies stipulating that employees comply with laws, regulations, and corporate policies as a condition of continued employment. In addition, employees are required to acknowledge ViaWest's stated values and confirm their commitment to upholding these values by performing their responsibilities in a professional and ethical manner. ViaWest employees are also required to report potential violations or exceptions to these policies that they suspect are being performed by another employee, contractor, or outsider.

Commitment to Competence

The competence of employees is a key element of the control environment. ViaWest is committed to developing its employees. This commitment to competence is expressed in the company's personnel policies and related human resource programs. Specific indicators of the commitment to personnel development include recruiting and hiring policies, investment in training and development, and performance monitoring.

ViaWest's commitment to competence begins with recruiting, which is the joint responsibility of the Human Resources Department and business unit managers. Hiring decisions are based on various factors, including education, prior relative experience, past accomplishments, and evidence of integrity and ethical behavior. In addition, prospective employees will go through reference and background checks before they are hired.

Assignment of Authority and Responsibility

The control environment is greatly influenced by the extent to which individuals recognize that they will be held accountable. This includes assignment of authority and responsibility for operating activities and establishment of reporting relationships and authorization protocols. Policies describing appropriate business practices, knowledge, and experience required of key personnel, and resources are communicated to employees for carrying out their duties.

Personnel Management Practices

The Human Resources Department communicates to employees expected levels of integrity, ethical behavior, and competence. Such practices relate to hiring, orientation, training, evaluation, counseling, promotion, compensation, and remedial actions.

ViaWest's approach to customer service begins with its staff. The organization has attracted and retained a diversified group of experienced professionals. ViaWest's hiring practices are designed to help ensure that new employees are qualified for their job responsibilities. ViaWest's hiring policies and guidelines assist in selecting qualified applicants for specific job responsibilities. Employee training is accomplished through supervised on-the-job training, formal in-house training courses, online learning, and external continuing education programs. Department managers are responsible for overseeing the training and development of qualified employees for current and future responsibilities.

Background checks are required for ViaWest employees, regardless of job function. Applicants first complete an application and an Authorization Check Form (for the background check). The background check is sent to a third-party vendor, which then runs Social Security, criminal (local, national, and federal), and Office of Foreign Assets Control (OFAC) checks; employment history verification; and a motor vehicle check on the individual. Credit checks are only conducted for potential employees in certain finance roles. Background checks are obtained prior to the finalization of an offer. In addition, offer letters mention that offers are pending satisfactory background and reference checks, in case an issue arises in the future.

Formal performance reviews are conducted on a regular basis. During these reviews, employees are evaluated based upon the responsibilities of their particular job and the values of the company. Employees are required to meet stated performance and attendance standards and to follow ViaWest's policies and procedures.

New hires meet with the Human Resources Department within their first two days and review new hire information, including the confidentiality agreement. If the agreement is not signed within 48 hours of hiring, the new employee cannot report to work until the document has been signed.

All ViaWest personnel are required to attend security training. Additional training in facilities operations, safety, and security is required for service support roles. A form illustrating required training must be completed, and management's approval for permanent access is required to document and track permanent data center access authorizations. Also, periodic security update training decks are created by management and distributed to employees.

Risk Management

ViaWest has placed into operation a risk assessment process to identify and manage risks that could affect ViaWest's ability to provide services to its customers. This process requires management to identify significant risks in its areas of responsibility and to implement appropriate measures to address these risks. Operations management meets monthly, or more frequently if necessary, to review the status of each area of the company's operations and to assess risks that could affect service delivery to its customers. Also, management holds weekly After Action Review Board (AARB) meetings to discuss any issues that occurred during the prior week and what improvements can be made in operations to help prevent the issue from occurring again. The meeting consists of team leads, managers, and directors from ViaWest's Operations group.

Information accumulated and discussed during monthly and AARB meetings is also fed into the other meetings that are held quarterly, such as the Quality, Security, and Compliance (QSC) Executive Governance Committee and QSC Management Governance Committee meetings. ViaWest created these committees to enable ViaWest to better identify risks, discuss remediation plans for identified risks, and develop action plans to remediate identified risks to help improve ViaWest's security and availability obligations to its customers. The meetings consist of individuals from various groups throughout the organization, but primarily consist of representatives from Legal, Security, Information Technology, Human Resources, Engineering, and Operations.

Information and Communication

ViaWest management is committed to maintaining effective communication with personnel and customers. To help align business strategies and goals with operating performance as it relates to customers, the Operations Management Team participates in weekly meetings in order to discuss the status of service delivery, capacity planning, quality performance, help desk statistics, and other matters of interest or concern.

The Executive Management Team meets monthly to discuss ViaWest's strategic initiatives and to address operational risks and concerns. The CEO meets with the team quarterly to review key performance metrics and strategic initiatives and to provide an overview of the company's performance to date.

In addition to the above communication methods, customers have been given access to ViaWest's internal ticketing systems, Cadence and Cerberus, through online portals MySupport and Client Center Portal, respectively. This provides customers the ability to report incidents and issues relating to their systems.

Control Activities

Internal controls are developed from the company's policies and procedures and help ensure management directives are carried out. They also help ensure that necessary actions are taken to address risks to the achievement of the entity's objectives. Controls, whether automated or manual, generally relate to the achievement of specific control objectives and are applied at various organizational and functional levels.

Specific control activities are provided in the *Control Environment* and *Overview of ViaWest's Colocation, Managed Services, and Client Center Cloud System* descriptions and in the *Description of Criteria, Controls, Tests, and Results of Tests* below.

Monitoring

Management and supervisory personnel monitor the quality of internal controls as part of their activities. ViaWest has implemented a series of management reports and metrics that measure the results of various processes involved in providing services to its customers. Some of the key metrics that the Operations Management Team monitors are as follows:

1. *Capacity:*
   - Power
   - Space
   - Cooling
   - Generator
   - Network
   - Servers
2. *Quality of Service:*
   - Network uptime
   - Backbone availability
   - Facility uptime
3. *Operations Center:*
   - Support call answer speeds
   - Support call volumes
   - Average talk time

The ViaWest Security, Operations, and Compliance Teams are responsible for implementing procedures and guidelines to identify the risks inherent in ViaWest's operations. The foundation of the risk management process is management's knowledge of its operations and its close working relationship with its customers. For any risks identified, management is responsible for implementing appropriate measures. Monitoring of risks is coordinated out of the Security, Operations, and Compliance Teams and reported during AARB, QSC Executive Governance Committee, or QSC Management Governance Committee meetings.

5 Description of Information Technology General Controls

This section provides a description of the controls performed by ViaWest specific to the System. These controls are designed to help ensure the proper authorization, accuracy, completeness, and timeliness of the functions mentioned below. All controls listed below related to policies, logical access for colocation services, physical security, change management, incident management, and environmental systems support all segments of the Colocation, Managed Services, and Client Center Cloud System. However, the controls listed below related to logical access for the Managed Services and Client Center Cloud environments are the incremental controls related to only those two segments of the system and are not applicable to the colocation portion of the system.

Policies

ViaWest has implemented policies and procedures to provide guidance to employees and contractors in performing their job functions and customer support activities in support of the ViaWest Colocation System. Policy and procedure documents are assigned to responsible directors or managers to manage, monitor and update. Policy and procedure owners are defined by management and documented within each individual policy and procedure document. The policy and procedure documents take into consideration, but are not limited to, the following:

- Identifying and documenting the security requirements of authorized users
- Assessing risks on a periodic basis
- Preventing unauthorized access
- Adding new users, modifying the access levels of existing users, and removing users who no longer need access
- Assigning responsibility and accountability for system security
- Assigning responsibility and accountability for system changes and maintenance
- Testing, evaluating and authorizing system components before implementation
- Addressing how complaints and requests relating to security issues are resolved
- Identifying and mitigating security breaches and other incidents
- Providing for training and other resources to support its system security policies
- Handling exceptions and situations not specifically addressed in its system security policies
- Providing for the identification of and consistency with applicable laws and regulations, defined commitments, service-level agreements and other contractual requirements
- Sharing information with third parties

ViaWest policies and procedures are reviewed and updated periodically. Policy or procedure changes can be enacted as a result of periodic review meetings, internal or external assessments, government or regulatory law revision, technological changes, or changes in industry-recognized leading practices. As policy changes are identified, the change is submitted, the policy is updated, and the policy owner reviews and approves the change. Last reviewed and last revised dates are maintained within each individual policy document, including the individual owner who approved the updated policy.

ViaWest management evaluates its organizational structure, reporting lines, authorities, and responsibilities as part of its business planning process and as part of its ongoing risk assessment and management process and revises these when necessary to help meet changing commitments and requirements. ViaWest includes a system description on its internet site. This description provides a broad overview of the Colocation, Managed Services, and Client Center Cloud System and the services it supports. Further detailed descriptions of the services and ViaWest's responsibilities are communicated to individual customers in brochures prior to onboarding and through the Client Guidebook and contracts during and after the customer onboarding process. ViaWest's responsibilities and customer responsibilities are clearly defined in such documents.

Included in the Client Guidebook are details that ViaWest customers need to enable them to communicate security or availability issues. The Client Guidebook details specific procedures on how to report such incidents and the mechanisms available to customers to report such incidents.

To help ViaWest personnel adhere to the commitments made to customers, ViaWest posts policies and procedures on the ViaWest corporate intranet for all employees to read. During the hiring process, employees are made aware of the policies and procedures and sign a form acknowledging their understanding of, and agreement to adhere to, such policies and procedures. Security awareness training is included as part of the onboarding process. Also, on a periodic basis, ViaWest distributes a security awareness and policy reminder notification. This communication details ViaWest's responsibilities as they relate to obligations to customers and locations of significant policies and procedures that reside on the corporate intranet.

During the onboarding process, written job descriptions are provided to potential candidates, and the hiring managers also interview potential candidates based on the written job descriptions to help ensure that appropriate personnel are hired and that the candidate fully understands the functions he or she will be performing. After the candidate is hired, the job description is maintained in the employee's permanent file for performance evaluation purposes.

New hires are informed of all ViaWest policies and procedures during the onboarding process. If the new hires will be in a customer support position, Engineering or any other function that will support the System, they are provided the ViaWest Incident Response Policy/Procedure to enable them to carry out their specific job functions. The ViaWest Incident Response Policy/Procedure is available on the ViaWest policy intranet site.

During the onboarding process, customers have the ability to customize how they receive communication from ViaWest. If customers have opted into email communication, they will be notified of service-affecting events.

Logical Access – Colocation Services

New or Modified User Access

Employees have access to ViaWest systems, applications, and network devices, with access-level restrictions based on specific job functions that the user performs for ViaWest.

New access to the network is initiated by the Human Resources Department. Access rights are assigned based on the function/role the Human Resources Department inputs into UltiPro for the new hire.

Access to network devices is controlled by the implementation of ACLs that limit where connections can be made from. Users authenticate to the network devices using TACACS+, which is administered via Cisco ACS. ACS leverages AD group membership to define permission levels in network devices, which are restricted by different group tier assignments. Access for a group tier is requested based on the necessity of the job function and must be approved by the employee's manager and the Compliance Department before access is granted.

RSA SecurID two-factor authentication is also used for authentication to the network devices. All users have unique usernames and PINs in addition to the token. Authentication tokens change on a fixed interval of 30, 60, or 120 seconds. PINs are not required to change on any fixed schedule.

Terminated Users

The Human Resources Department initiates the employee termination process and revokes the employee's logical access to ViaWest's network accounts. The Human Resources Department or the employee's supervisor conducts an exit interview with the terminated employee and collects physical access tokens. A termination notification is generated for relevant departments to authorize access revocations from other ViaWest facilities, network devices, and systems.

User Access Reviews

To help ensure that access to systems, applications, and network devices remains authorized and appropriate over time, management performs user logical access reviews on users who have access to the corporate domain and network devices. This review consists of inspecting the entire user base to verify that no terminated employees have access to the systems and to verify that users' current access rights are still required and appropriate based on job changes or roles they are currently fulfilling within the organization. Any exceptions identified by management are sent to the Logical Access Administrators of the respective systems for resolution, and the changed access lists are revalidated for completion of the review by management.

Privileged User Access

Administrative access to network devices is commensurate with job function and is limited to the Engineering and Production Support Teams. In order to access the network devices, ViaWest has created ACLs on each device to allow only certain IP addresses to connect to the device. The user must also be defined to a specific group within TACACS+ in order to administer the network devices. Authentication to TACACS+ is controlled through Cisco Secure ACS.

Password Controls and Security

Access to the network and supporting tools (i.e., the ticketing system) within the colocation environment is restricted by using password authentication guidelines requiring that passwords be a minimum length, conform to complexity requirements, expire periodically, and differ from a previous number of passwords to help prevent unauthorized access.

The network devices are accessed from ViaWest-approved IP addresses. The IP addresses are defined on each network device through the use of ACLs. After a user connects to the device from an authorized IP address, the user must authenticate to the device using his or her TACACS+ credentials. The TACACS+ servers require a username, PIN, and token in order to access the network device.

Logical Access – Managed Services and Client Center Cloud

Access to resources within the Managed Services environment is controlled via Windows Active Directory domain membership. To access client servers, ViaWest personnel are assigned access to Windows groups or a shared account, which are then assigned rights on client servers. To access client network devices and firewalls, ACLs on each device restrict access to allow only certain IP addresses the ability to connect to the device. The user must also be defined to a specific AD group configured on the ACS tool in order to administer the network devices using Radius. These

configurations are defined on each network device. Access to the ViaWest Customer Portal is granted via membership within Cadence, which for ViaWest employees use authentication via the ViaWest Managed Services domain.

Access to resources within the Client Center Cloud environment is also controlled via Windows Active Directory domain membership. To access client servers, ViaWest personnel are assigned access to either a domain group for Windows servers, or are assigned a PKI for Linux servers. To access network devices and firewalls, users must be granted access on the TACACS server. However, all configurations on client servers, network devices, and firewalls in the Client Center Cloud are controlled by Puppet.

Access to the Client Center Portal is granted via membership within either the Client Center Cloud corporate domain or Conflux, which utilizes Client Center Cloud corporate domain AD groups.

New User Access

Permission levels on the Managed Services and Client Center Cloud domains are further restricted by different group assignments. Access to the domains is based on the necessity of the job function and must be approved by the employee's manager and/or the Compliance Department before access is granted.

Terminated Users

The Human Resources Department initiates the employee termination process and revokes the employee's logical access to the ViaWest corporate domain, the Managed Services domain, and the Client Center Cloud client domain, which effectively disables access to all other tools and resources impacting client environments. A termination notification is generated for relevant departments to authorize access revocations from these systems.

Privileged User Access and Client Server Access

Administrative access to the Managed Services domain, Customer Portal (via Cadence), and firewall devices to Radius (the Managed Services firewall device administration application), to ACS (the authentication tool used for Radius), to the Client Center Cloud domains, to Puppet, and to Net Line Dancer is commensurate with job function and is limited to the Engineering and Production Support Teams.

For Managed Services, customer servers utilize either a customer-managed domain or the Managed Services domain. Administrative access to servers on customer-managed domains is controlled by the customer and the customer is responsible for administering account access to ViaWest. Administrative access to servers managed on the ViaWest Managed Services domain is controlled by ViaWest, and access is restricted through domain group membership.

For the Client Center Cloud, customer servers utilize the Client Center Cloud client domain. Administrative access to Windows servers on this domain is limited to users in a restricted Active Directory group. Administrative access to Linux servers is controlled via Public Key Infrastructure, and keys are granted to a limited number of Linux engineers who require access to maintain the servers.

User Access Reviews

To help ensure that access to client systems related to Managed Services remains authorized and appropriate over time, management performs semiannual user logical access reviews on users who have access to the Managed Services domain, Radius, and the Customer Portal (via Cadence Access). To help ensure that access to client systems related to the Client Center Cloud remains authorized and appropriate over time, management performs quarterly logical access reviews over users with access to client Windows and Linux servers.

These reviews consist of inspecting membership to the user bases along with key groups to verify that no terminated employees have access to the systems, and to verify that users' current access rights are still required and appropriate based on job changes or roles they are currently fulfilling within the organization. Any exceptions identified by management are sent to the Logical Access Administrators of the respective systems for resolution, and the changed access lists are revalidated for completion of the review by management.

Password Controls and Security

Access to the Managed Services domain and Client Center Cloud domains and supporting tools (Radius, Customer Portal, Client Center Portal, Puppet, Conflux, Cerberus, Nagios, Net Line Dancer) is restricted by using password authentication guidelines requiring that passwords be a minimum length, conform to complexity requirements, expire periodically, and differ from a previous number of passwords to help prevent unauthorized access.

Managed Services: Customer-Specific Firewall Security

Customer-specific firewall devices are used within the Managed Services environment. The IP addresses are defined on each device through the use of firewall policies. Each customer firewall is configured with ViaWest's default policies and configurations, which restrict access to the minimum monitoring tools and operations personnel necessary. For a change to be made to a customer firewall configuration, a ticket is created and must be approved by the customer before the change is implemented, whether during initial customer onboarding or subsequent to onboarding.

Client Center Cloud: Network Device and Server Security

Access to client servers and network devices, including firewalls, is restricted to limited personnel as noted above. In addition, any changes made by these personnel are overwritten every 30 minutes by the master configuration files for that device as stored in the Puppet tool. The Puppet tool is configured to generate alerts for any device that was not updated during the last two scans.

Physical Security

General Physical Security

Physical security of the data centers is the responsibility of data center customer support (DCCS) personnel, along with coordination by Security and members of senior management. Physical access to ViaWest locations is monitored by VTAC and DCCS personnel 24x7.

Physical access to each of the ViaWest data centers is controlled through various preventative measures. To help ensure that only authorized employees, customers, or vendors have access to the data centers, ViaWest has implemented electronic card key systems. In order for any one individual to access the raised floor area, the individual must have a valid and approved access card for that specific data center. After an individual scans his or her card, the individual must also have knowledge of the PIN or the correct biometric reading associated with the badge in order to gain entry to the raised floor area.

After an individual authenticates to the raised floor area, he or she must also have access to the customer's equipment through the use of another lock and key, PIN, or biometric reader. Each customer is allocated his or her own space through the use of secured racks, cages, or suites.

All data center physical access activity is monitored through various monitoring systems. Each ViaWest data center has security cameras installed to monitor and record physical access events. Data is recorded based on activity/motion, up to available memory capacity. The standard data retention period for key areas is 90 days, but may vary slightly between ViaWest data center locations due to activity captured and capacity. Data center doors also have monitoring systems in place to alert DCCS personnel regarding doors that remain open too long, doors that are forced open, or doors that are opened that should remain closed. DCCS personnel also monitor physical activity throughout each data center since all camera activity is fed into the Operations Center.

DCCS personnel perform observation rounds of each data center throughout each day to physically inspect each data center's building exterior, docks, storage facilities, security cameras, and security systems. This helps to ensure that physical security systems are operating as designed.

General Physical Security – Client Center Cloud

Physical security at the Westin and Equinix data centers is the responsibility of each subservice organization (SSO). On an annual basis, ViaWest personnel obtain and review a listing of all ViaWest users with access to the SSO's data centers. ViaWest notifies the SSO of any necessary access changes identified during the review.

New or Modified Employee Physical Access

All ViaWest personnel are required to attend security training. Additional training in facilities operations, safety, and security is also required for service support roles. A form illustrating that required training has been completed, along with management's approval for physical access, is required in order for an employee to gain data center access.

Vendor and Customer Access

To authorize access for a vendor, a Vendor Access List (VAL) form must be completed. This form must be approved by a ViaWest vice president who is a member of the Operations or Executive Management Teams or a data center manager and the vendor's Single Point of Contact (SPOC). The badge issued in response to the approved VAL form will allow the vendor access to the data center locations specified on the VAL form.

Each customer must identify the individuals (employees or third-party vendors) who are authorized to access ViaWest facilities on its behalf. Authorized access is managed through the customer's MySupport Portal account by a customer-designated user administrator, who accesses the MySupport Portal and specifies an individual as authorized to access facilities on the customer's behalf. Authorization may be for either a permanent access badge or a day pass only. The MySupport system generates a ticket for ViaWest DCCS staff to act upon for each occurrence. The same process applies for revoking access.

For both vendors and customers, the requested data center does not generate the badge until the requested user arrives on-site. After arriving on-site, the user is provided a copy of ViaWest's data center rules. In order to obtain an access badge, the user must present a valid government-issued picture ID and sign a Customer or Vendor DC Access Card Receipt and Acknowledgement form, acknowledging and agreeing to the rules of the data center.

Physical Security Access Reviews

Physical access reviews are performed quarterly to help ensure that only authorized employees, vendors, and customers maintain access to the ViaWest data centers. Physical access lists are generated from each data center and are compared to current employee-, customer-, and vendor-authorized access lists. Any exceptions noted are recorded and tracked to resolution.

Additionally, management performs logical access reviews on users who have administrative access to the various physical access badging systems. This review consists of inspecting the user base of administrators to verify that no terminated employees have access to the systems and to verify that users' current access rights are still required and appropriate based on job changes or roles they are currently fulfilling within the organization. Any exceptions identified by management are sent to the administrators of the respective systems for resolution, and the changed access lists are revalidated for completion of the review by management.

Customer Cage Access

Within each data center, customer environments are physically secured within a locked cage, cabinet, or suite. Customer cabinets and cages are secured by keyed locks (keys secured via lock box), combination locks, card readers, biometric devices, and/or keypads per the customer's choice.

Master keys are kept in a secure environment not accessible to customers or vendors. Operational vice presidents are authorized to have master keys and DCCS personnel are required to carry master keys, as are data center managers and their direct reports (i.e., those who perform customer installations).

Change Management

Maintenance Windows

Network changes that are known to, or have the potential to, affect customer services are placed in a scheduled maintenance window. Weekly time frames are set aside in case maintenance is necessary. If a maintenance window is necessary outside of the time frame set aside each week,

ViaWest management approves the maintenance window using the maintenance window in ViaWest's proprietary Maintenance Window system. The outage is also posted on the ViaWest Customer Support Portal, MySupport.com.

Non-routine changes are tested in a test lab and approved by the Vice President of Network Operations. To minimize network device configuration problems, RANCID and Net Line Dancer are utilized to create snapshots of each device configuration. RANCID is used for Colocation and Managed Services devices and Net Line Dancer is used for the Client Center Cloud devices. Each night, both tools pull the device configurations in order to have an updated "snapshot" of the device configurations.

Daily, RANCID and Net Line Dancer generate email notifications of any device configurations that have changed since the previous day's snapshot of configurations. These email notifications go to the Network Operations Team, which reviews these emails to verify that appropriate activity is occurring on the network devices.

Monitoring and Incident Management

ViaWest has implemented monitoring controls at all of its data centers to enable monitoring of critical environmental systems, customer systems, and the hosting network. Tools are used to monitor these critical systems. If issues are identified, other tools are used to track and remediate any incidents that occur. All data centers are monitored 24x7 by DCCS and VTAC personnel.

Management has also implemented other controls to review incidents that occurred during a given month to determine whether there are any trends, security, or availability issues that may need greater attention.

In order to monitor systems and provide for system stability, data centers are monitored 24x7. The Hillsboro, Portland; Arapahoe, Denver; Champa, Denver; Wazee, Denver; Cornell, Denver; Compark, Denver; Delong, Salt Lake City; Synergy Park, Dallas; Carson, Las Vegas; Lone Mountain, Las Vegas; Phoenix; Minneapolis; Dallas Infomart; Plano; Allentown; and Calgary Network Operations Centers are staffed with ViaWest DCCS personnel on-site, 24x7. Additionally, all data centers have building management systems that provide alarming of all critical infrastructure equipment.

The Lindon, Cottonwood, and Presidents data centers have an on-site Operations Center; however, they are not staffed 24x7. During hours when they are not staffed on-site, they are monitored by personnel at the Delong DCCS using the building management system, Nimbus alert system, the data center's card access system, and a system that provides direct visual feeds from security cameras.

The Austin data center does not have an on-site Operations Center. Instead, on-site personnel monitor the data center during normal business hours. During hours when this data center is not staffed on-site, it is monitored by DCCS personnel at the Dallas location. The data center uses building management systems that provide monitoring and alarming.

Monitoring and Alert Systems

ViaWest employs tools for monitoring and alerting of environmental systems, servers, services, and network devices. Checks performed of the ViaWest environment by the Nimbus monitoring tool include both internal and external checks. External checks permit ViaWest to monitor services where the system queries the target server from the outside. Internal checks, where the monitored system is evaluated from inside the target system itself, allow for significantly more detailed monitoring data points. Common checks are CPU utilization and log messages, which can be configured to trigger an alarm notification.

ViaWest employs a building management system (BMS) in several of its data centers to monitor the status of key environmental systems, including SetPoint and the BMS Monitoring and Control System. For those data centers that do not have an integrated BMS, each of the key environmental systems is configured with a dry contact that alerts the Operations Center if the system is not functioning as intended.

The ViaWest monitoring tools are distributed across many facilities and consist of numerous systems. This permits monitoring to occur as close to the target systems as possible. Easy access to the current state of monitored systems is accessible via the tool's web-based status interface. ViaWest DCCS personnel continuously display this interface to stay abreast of the overall health of the monitored systems and devices.

The monitoring tools have been implemented to automatically trigger events (ticket creation and staff notification) directly in the ViaWest ticketing system and via phone/email. This integration between the ticketing system and the monitoring tools allows alarms to be automatically assigned to the appropriate on-call individual for resolution.

Incident Management

The ViaWest ticketing systems use information from the monitoring tools for both customer and internal devices. There is a dedicated DCCS staff 24x7 responsible for addressing alerts displayed within the application.

For Colocation and Managed Services, the Cadence ticketing system can be assigned a priority 0 through 5. The priorities are as follows:

- A priority 0 ticket is received via the monitoring tool and is defined as not yet evaluated by an engineer so as to be assigned the appropriate priority going forward. The priority 0 queue is monitored 24x7, and tickets are immediately evaluated and assigned the appropriate priority level by Solutions Engineers within the Operations Center.
- A priority 1 ticket is defined by an event that affects multiple customers. These tickets are opened manually by specific individuals. When appropriate, an Incident Response Team (IRT) conference call is convened by DCCS personnel with senior leadership to discuss impact and plans to mitigate or solve.
- A priority 2 ticket is defined by an event where a single customer environment is down or critically affected. If there is continuous downtime for 60 minutes, senior management is paged and notified of the downtime. Senior management then contacts the DCCS to discuss the resolution plan.

- A priority 3 ticket can be created by a Solutions Engineer if it is determined that the event is urgent, but not a customer-down event.
- Priority 4 tickets are reserved for customer questions.
- Priority 5 tickets are reserved for project work.

For the Client Center Cloud, the Cerberus ticketing system contains the following priority types:

- Site Down: for occasions when the hosted site or cloud application is completely down
- Urgent Need: for time sensitive needs that require a change or an adjustment to keep the site functioning correctly
- Support Request: all other needs

For the Client Center Cloud, notifications are configured to alert ViaWest management in the event that a Site Down ticket has not been responded to within the first minute.

A customer can prioritize its tickets based on the impact to its business. A customer is notified depending on the priority and surrounding situation. If a customer is required to be notified, an Account Manager (or his/her backup) contacts the customer to discuss resolution.

When a customer issue arises, ViaWest Account Management is notified in one of several ways: ticket notifications through Cadence, email, or a direct phone call from DCCS staff. The Account Management Team will contact the customer as necessary while the on-call staff works to resolve the issue as quickly as possible.

Work related to a customer-initiated problem ticket is performed on customer systems as requested by authorized customer representatives over the phone or utilizing the customer's MySupport or Client Center Portal.

ViaWest Management Meetings

ViaWest management holds several meetings to discuss and resolve issues related to data center operations, uptime, network availability, risks identified in the business, and any issues or other information that relates to data center operations. The meetings include the monthly Capacity meetings and the weekly AARB meetings.

Third-Party Tools and Assessments

In order to monitor the ViaWest System, ViaWest engages independent third-party auditors to periodically assess the components of its System. Issues identified during such audits are recorded, tracked and remediated to improve the overall system and to help ensure that ViaWest is meeting its obligations to customers. ViaWest also incorporates the use of third-party tools to perform vulnerability scans on internet-facing applications. Corporate Security Scans are performed monthly and the results are sent to the internal IT Team, which is responsible for investigation and remediation efforts. The Customer Support Portal is scanned each weekend. These results are sent to the Development Team for investigation and remediation.

Environmental Systems

ViaWest data centers are equipped with environmental systems to help ensure that customer systems are available, protected, and monitored.

Each data center is equipped with UPS and generator systems to help ensure that data centers are supported by redundant power sources so that customer systems remain available. Each UPS device is configured to provide sufficient power to support the entire data center until the generator engages to provide continued power. Each generator maintains an appropriate fuel supply, and each data center contracts with a third-party fuel provider to refuel the tanks as necessary.

Data centers are also equipped with HVAC systems. Each data center is supported by a sufficient number of HVAC systems to allow for N+1 cooling redundancy on the raised floor.

Each data center is equipped with fire monitoring and prevention systems and fire extinguishers throughout the facility.

All environmental systems are monitored by ViaWest systematically and by visual inspection.

Recurring Site Inspections

Every day, site personnel periodically perform physical inspections of staffed data centers to verify that all critical systems and access security solutions are operational and that environmental operating conditions remain within acceptable ranges. If a deviation is observed, the technician will log the event and create a trouble ticket for corrective actions.

Generator Testing and Inspections

All generators are subject to one annual preventative maintenance procedure. In addition, all generators are engaged for start-up and run operation at least once per month. Operating results are logged, and any issues are noted for follow-up and timely resolution.

Power Management and Semiannual UPS Inspections

Power management equipment is in place at each data center for:

- A dedicated utility step-down transformer
- An automatic transfer switch that is connected to standby diesel generators

The mission-critical electrical loads at each data center are sourced by UPS systems. In addition, semiannual preventative maintenance procedures are performed on all UPS systems and batteries.

ViaWest also contracts with an outside vendor to perform annual infrared scans of all power distribution unit (PDU) systems. Any issues identified during the annual inspection are recorded for follow-up and resolved.

Fire Detection and Suppression Equipment and Inspections

Fire detection and suppression equipment is installed in all data centers. Annual fire inspection and preventative maintenance procedures are performed to confirm that the detection and suppression equipment is operating within optimal ranges.

HVAC Equipment

Each data center has an adequate supply of cooling capacity to support cooling requirements in the event of a loss of any critical cooling component.

Preventative maintenance is performed every three months, at a minimum, on all cooling equipment. Building management systems alarm and notify data center managers if humidity or temperature thresholds are breached.

Maintenance windows are opened and approved by authorized personnel prior to performing any necessary repairs and maintenance.

Network Availability

Each data center maintains redundant links to the internet and other ViaWest data centers. Devices are configured to be monitored in the monitoring tool and are not accessible for management access outside the ViaWest network. Additionally, the network design supports redundancy for critical network components, and 24x7 monitoring procedures are in place to monitor ViaWest and customer systems. Monitoring systems are redundant to provide failover capability, and current network diagrams are available for use by authorized users.

Environmental Systems – Client Center Cloud

Environmental systems at the Westin and Equinix data centers are the responsibility of each subservice organization.

Backups

All ViaWest network devices are backed up nightly. ViaWest uses RANCID and Net Line Dancer to track changes to the network device configurations and maintain the most up-to-date copies of the configurations.

ViaWest uses EMC Avamar and BSM for monitoring client server backups. These tools are configured to alert ViaWest personnel via Cadence (for Managed Services) or via Nagios (for Client Center Cloud). ViaWest personnel then work in tandem with clients to resolve the root cause of the issue so that backups can be completed successfully going forward. All backups are replicated to a secondary data center within the ViaWest environment.

Trust Services Criteria and Controls

The trust services criteria for security and availability, and the controls that meet those criteria, are listed in the accompanying *Description of Criteria, Controls, Tests and Results of Tests.*

Complementary User Entity Controls

In designing its system, ViaWest has detailed certain controls that should be implemented by user entities to meet the applicable criteria. Those control considerations are documented below:

- User entities are responsible for having controls in place to help ensure that access to server operating systems, network operating systems, databases, and application systems located on the user entities' servers or domains are appropriate.
- User entities are responsible for maintaining their own firewall and network security controls.
- User entities should regularly review employees with physical access to ViaWest data centers for appropriateness. Any changes to employees with privileged access should be communicated to ViaWest in a timely manner.
- User entities are responsible for designating account administrators for the purpose of maintaining their authorized contact and physical access lists.
- User entities are responsible for maintaining the ongoing validity of their authorized contacts through ViaWest's Customer Support Portal.
- User entities are responsible for having controls in place to help ensure that changes to server operating systems, network operating systems, databases and application systems located on the user organization's servers are appropriate.
- User entities are responsible for confirming that service requests made to ViaWest are completed successfully and within an appropriate time frame.
- User entities are responsible for confirming that backups are configured according to their requirements.
- User entities are responsible for ensuring that backup failures are resolved in a timely manner.

Complementary Subservice Organization Controls

In designing its system, ViaWest has contemplated that certain complementary controls would be implemented by its subservice organizations to achieve the applicable criteria included in this report. Those control considerations are documented below:

- Subservice Organizations are responsible for ensuring that data center access for their employees, contractors, vendors, and clients is added only for authorized individuals.
- Subservice Organizations are responsible for ensuring that data center access for their employees, contractors, vendors, and clients is removed in a timely manner when no longer required.
- Subservice Organizations are responsible for implementing physical access mechanisms to ensure only authorized badge holders can enter the data centers.
- Subservice Organizations are responsible for ensuring customer-specific areas within the data center can only be accessed by the customer.
- Subservice Organizations are responsible for performing environmental preventative maintenance activities on their emergency power systems, fire protection systems, and heating and cooling systems.

SECTION IV. DESCRIPTION OF CRITERIA, CONTROLS, TESTS AND RESULTS OF TESTS

1 Testing Performed and Results of Tests of Entity-Level Controls

In planning the nature, timing, and extent of our testing of the controls specified by ViaWest, we considered the aspects of ViaWest's control environment, risk assessment processes, information and communication, control activities, and management monitoring procedures and performed such procedures as we considered necessary in the circumstances.

* * * * *

On the pages that follow, the controls have been specified by, and are the responsibility of, ViaWest. The testing performed and the results of tests are the responsibility of Ernst & Young LLP. The testing performed was conducted across all ViaWest facilities; however, physical site observations for this report were only conducted at two data centers in Denver, Colorado; one in Hillsboro, Oregon; one in Salt Lake City, Utah; one in Phoenix, Arizona; one in Austin, Texas; two in Dallas, Texas; one in Las Vegas, Nevada; and one in Allentown, Pennsylvania.

Testing of Information Produced by the Entity

For tests of controls requiring the use of information produced by the entity (e.g., controls requiring system-generated populations for sample-based testing), we perform a combination of the following procedures where possible based on the nature of the information produced by the entity to address the completeness, accuracy, and data integrity of the data or reports used: (1) inspected the source of the information produced by the entity; (2) inspected the query, script, or parameters used to generate the information produced by the entity; (3) tied data between the information produced by the entity and the source; and/or (4) inspected the information produced by the entity for anomalous gaps in sequence or timing to determine the data is complete and accurate. Furthermore, in addition to the above procedures, for tests of controls requiring management's use of information produced by the entity in the execution of the controls (e.g., periodic reviews of user access listings), we inspected management's procedures to assess the validity of the source and the completeness, accuracy, and integrity of the data or reports.

Common Criteria Related to Organization and Management

CC1.1 The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system enabling it to meet its commitments and system requirements as they relate to security and availability.	
Controls specified by ViaWest, Inc.	**Tests performed**
SEC2.03B: Changes and updates to system policies and procedures are communicated to entity personnel through email and are placed on the ViaWest intranet to be available to all entity personnel.	Inquired of the Director of Compliance to determine whether employees were informed of policy and procedure changes and whether employees were notified through email or through updates on the corporate intranet. Inspected email evidence to determine whether updates to policies and procedures were communicated to ViaWest personnel. Inspected the ViaWest intranet site to determine whether policies and procedures were available to ViaWest personnel.
SEC3.11A: ViaWest has defined job descriptions for each employee to help assign personnel to the appropriate role and to evaluate applicants based on the role they will be performing for the organization.	Identified a population of new hires within the UltiPro HR system during the period, selected a sample of new hires, and inspected the employee's HR file to determine whether: • The individual's job description was included in the employee's HR file • The queries used to generate the listings from UltiPro contained the appropriate selection criteria Inspected a sample of job descriptions maintained by HR for a sample of current employees to determine whether job descriptions exist for current employees.
CC1.1C: Management evaluates its organizational structure, reporting lines, authorities, and responsibilities as part of its business planning process and as part of its ongoing risk assessment and management process. Management revises these when necessary to help meet changing commitments and requirements.	Inspected the current organizational chart to determine whether it had been reviewed and updated within the current year. Inquired of the Director of Compliance and inspected email to determine whether responsibilities and authorities were assessed as a result of personnel changes.
Results of Tests: No deviations noted.	

Common Criteria Related to Organization and Management

CC1.2 Responsibility and accountability for designing, developing, implementing, operating, maintaining, monitoring, and approving the entity's system controls and other risk mitigation strategies are assigned to individuals within the entity with authority to ensure policies and other system requirements are effectively promulgated and implemented to meet the entity's commitments and system requirements as they relate to security and availability.	
Controls specified by ViaWest, Inc.	**Tests performed**
SEC1.01A: ViaWest policies and procedures are established, and responsibility for the policies and procedures is defined and assigned to specific policy owners, the CSO and compliance.	Inquired of the Director of Compliance to determine whether responsibility for the maintenance of ViaWest policies and procedures was established and defined. Inspected policy and procedure documents to determine whether they existed and provided guidance for employees in managing the activities of the business.
SEC1.01B: ViaWest policy and procedure documents are reviewed and updated by assigned parties and policy owners as needed. Updates to the policies are noted within the policy. An update date and reviewer/approver are identified within the policies and procedures.	Inquired of the Director of Compliance to determine whether management periodically reviewed and updated policy and procedure documents throughout the course of the examination period. Inspected a sample of policy and procedure documents to determine whether assigned parties and policy owners for the selected policies and procedures reviewed and approved any updates to the documents.
CC1.2C: Responsibility for each system control has been assigned to a member of management. On an annual basis, the control owners review the control to determine whether the control addresses the risks of the current system requirements.	Inspected the listing of controls in the master control matrix to determine whether each control was assigned a control owner. For a sample of controls, inspected job titles and email evidence to determine whether the owner was appropriate based on his/her job responsibilities, the owner reviewed and approved the current control, and any changes identified were subsequently identified and communicated.
Results of Tests: No deviations noted.	

Common Criteria Related to Organization and Management

CC1.3 The entity has established procedures to evaluate the competency of personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring the system affecting security and availability and provides resources necessary for personnel to fulfill their responsibilities.	
Controls specified by ViaWest, Inc.	**Tests performed**
SEC2.02A: ViaWest employees must complete security awareness training during their onboarding process and acknowledge participation in the training and receipt of appropriate logical access, physical access and password security policies through sign-off on the appropriate acknowledgement form.	Identified a population of new hires within the UltiPro HR system during the period, selected a sample of new hires, and inspected the employee's HR file to determine whether: • The employee completed his or her security awareness training and he or she signed the acknowledgement form indicating completion of the training and receipt of required policies • The queries used to generate the listings from UltiPro contained the appropriate selection criteria
SEC2.02C: On an annual basis, ViaWest management creates a security awareness communication and sends it to all employees to review.	Inspected the annual security awareness training communication to determine whether all employees received the communication.
SEC3.11A: ViaWest has defined job descriptions for each employee to help ensure that personnel are assigned to the appropriate role and to evaluate applicants based on the role they will be performing for the organization.	Identified a population of new hires within the UltiPro HR system during the period, selected a sample of new hires, and inspected the employee's HR file to determine whether: • The individual's job description was included in the employee's HR file • The queries used to generate the listings from UltiPro contained the appropriate selection criteria Inspected a sample of job descriptions maintained by HR for a sample of current employees to determine whether job descriptions exist for current employees.
Results of Tests: No deviations noted.	

Common Criteria Related to Organization and Management

CC1.4 The entity has established workforce conduct standards, implemented workforce candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and system requirements as they relate to security and availability.	
Controls specified by ViaWest, Inc.	**Tests performed**
EL1: Background checks are performed when hiring new personnel.	Identified a population of new hires within the UltiPro HR system during the period and selected a sample of new hires. Inspected the employee's HR file to determine whether: • A background check was performed prior to the start of employment • The queries used to generate the listings from UltiPro contained the appropriate selection criteria
CC1.4B: Personnel are required to read and accept the code of conduct upon being hired. On an annual basis, personnel are required to reaffirm acknowledgement of the code of conduct within the employee handbook.	Identified a population of new hires within the UltiPro HR system during the period, selected a sample of new hires, and inspected the employee's HR file to determine whether: • The code of conduct was acknowledged during the onboarding process • The queries used to generate the listings from UltiPro contained the appropriate selection criteria
Results of Tests: No deviations noted.	

Common Criteria Related to Communications

CC2.1 Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external system users to permit users to understand their role in the system and the results of system operation.	
Controls specified by ViaWest, Inc.	**Tests performed**
SEC2.01A: ViaWest system and service descriptions are maintained on its external website. Such descriptions are available to current and potential system users.	Inspected the system description to determine whether it was developed and whether it was sufficient and appropriate per Trust Services requirements and against our understanding of the ViaWest Colocation System. Observed online that an appropriate system description is available on the ViaWest website.
SEC2.01B: ViaWest describes the description of the specific services provided to each customer in each individual customer contract and agreement.	Inquired of the Director of Compliance to determine whether customers were provided contracts during their onboarding activities. Identified a population of new customers using a customer report from the SugarCRM application. For a sample of new customers, inspected customer contracts and master service agreements to determine whether: • Such documents contained an appropriate description of the services and obligations • The query used to generate the listing from the SugarCRM application contained the appropriate selection criteria
Results of Tests: No deviations noted.	

Common Criteria Related to Communications

CC2.2 The entity's security and availability commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal users to enable them to carry out their responsibilities.	
Controls specified by ViaWest, Inc.	**Tests performed**
SEC2.01A: ViaWest system and service descriptions are maintained on its external website. Such descriptions are available to current and potential system users.	Inspected the system description to determine whether it was developed and whether it was sufficient and appropriate per Trust Services requirements and against our understanding of the ViaWest Colocation System. Observed online that an appropriate system description is available on the ViaWest website.
SEC2.01B: ViaWest describes the specific services provided to each customer in each individual customer contract and agreement.	Inquired of the Director of Compliance to determine whether customers were provided contracts during their onboarding activities. Identified a population of new customers using a customer report from the SugarCRM application. For a sample of new customers, inspected customer contracts and master service agreements to determine whether • Such documents contained an appropriate description of the services and obligations • The query used to generate the listing from the SugarCRM application contained the appropriate selection criteria
SEC2.03B: Changes and updates to system policies and procedures are communicated to entity personnel through email communication and are placed on the ViaWest intranet to be available to all entity personnel.	Inquired of the Director of Compliance to determine whether employees were informed of policy and procedure changes and whether employees were notified through email or through updates on the corporate intranet. Inspected email evidence to determine whether updates to policies and procedures were communicated to ViaWest personnel. Inspected the ViaWest intranet site to determine whether policies and procedures were available to ViaWest personnel.
Results of Tests: No deviations noted.	

Common Criteria Related to Communications

CC2.3 The responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties.	
Controls specified by ViaWest, Inc.	**Tests performed**
SEC2.02A: ViaWest employees must complete security awareness training during their onboarding process and acknowledge participation in the training and receipt of appropriate logical access, physical access and password security policies through sign-off on the appropriate acknowledgement form.	Identified a population of new hires within the UltiPro HR system during the period, selected a sample of new hires, and inspected the employee's HR file to determine whether: • The employee completed his or her security awareness training and signed the acknowledgement form indicating completion of the training and receipt of required policies • The queries used to generate the listings from UltiPro contained the appropriate selection criteria
SEC2.02B: ViaWest management posts all current policies on its corporate intranet site. All employees have access to these policies and procedures and are encouraged to review them in performing their job functions.	Observed the ViaWest corporate intranet site to determine whether management posted current policies and procedures on its intranet.
SEC2.02C: On an annual basis, ViaWest management creates a security awareness communication and sends it to all employees to review.	Inspected the annual security awareness training communication to determine whether all employees received the communication.
SEC2.03A: For all policies and procedures, ViaWest has designated a policy owner who is responsible for reviewing and approving updates to policies and procedures.	Inspected a sample of ViaWest policies and procedures to determine whether a policy owner was defined and had approved the policy or procedure.
SEC2.03B: Changes and updates to system policies and procedures are communicated to entity personnel through email and are placed on the ViaWest intranet to be available to all entity personnel.	Inquired of the Director of Compliance to determine whether employees were informed of policy and procedure changes and whether employees were notified through email or through updates on the corporate intranet. Inspected email evidence to determine whether updates to policies and procedures were communicated to ViaWest personnel. Inspected the ViaWest intranet site to determine whether policies and procedures were available to ViaWest personnel.
Results of Tests: No deviations noted.	

Common Criteria Related to Communications

CC2.4 Information necessary for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the security and availability of the system, is provided to personnel to carry out their responsibilities.	
Controls specified by ViaWest, Inc.	**Tests performed**
SEC3.07A: Representatives from ViaWest Operations, Data Center Services, VTAC, Service Delivery, Managed Services, Network Engineering, Client Relationship Management, and Business Controls and Compliance groups meet weekly during the After Action Review Board (AARB) meeting to evaluate, analyze, and define plans as necessary to discuss any issues that have disrupted service to customers. If a risk is identified, a project plan is created, resulting in changes.	For a sample of weeks, inspected calendar entries and meeting minutes to determine whether management scheduled and held the AARB meeting and representatives from the various groups were invited and attended. Inspected the AARB tracking document to determine whether management documented issues and resolutions within the document on an ongoing basis.
SEC1.01B: ViaWest policy and procedure documents are reviewed and updated by assigned parties and policy owners as needed. Updates to the policies are noted within the document. An update date and reviewer/approver are identified within the policies and procedures.	Inquired of the Director of Compliance to determine whether management periodically reviewed and updated policy and procedure documents throughout the course of the examination period. Inspected a sample of policy and procedure documents to determine whether assigned parties and policy owners for the selected policies and procedures reviewed and approved any updates to the documents.
Results of Tests: No deviations noted.	

Common Criteria Related to Communications

CC2.5 Internal and external users have been provided with information on how to report security and availability failures, incidents, concerns, and other complaints to appropriate personnel.	
Controls specified by ViaWest, Inc.	**Tests performed**
SEC2.04A: The process for customers and external users to inform ViaWest of possible issues and other incidents is posted on the Customer Portals.	Inspected the ViaWest Customer Portals to determine whether customers were provided with multiple support options for communicating security and related availability issues.
SEC2.04B: Documented procedures exist to identify and escalate system incidents.	Inspected the Problem Resolution and Escalation Policy and the Incident Management procedures document to determine whether identification and escalation procedures were in place.
SEC2.04C: Incident response procedures are available to all ViaWest employees through the ViaWest intranet site.	Inspected the ViaWest intranet site to determine whether internal escalation and contact policies and procedures were available to ViaWest personnel. Inspected the Information Security Policy to determine whether it included instructions for employees to report potential incidents.
Results of Tests: No deviations noted.	

Common Criteria Related to Communications

CC2.6 System changes that affect internal and external users' responsibilities or the entity's commitments and system requirements relevant to security and availability are communicated to those users in a timely manner.	
Controls specified by ViaWest, Inc.	**Tests performed**
SEC2.05A: ViaWest communicates changes to customers when a change may affect the customer's environment and the customer has requested to be notified of such changes.	Inspected the Problem Resolution and Escalation Policy to determine whether management is notified in the event of a system issue and whether management procedurally notifies customers of service/security impacting issues. Inspected the log of communications for a sample of customer-impacting changes from the population of Maintenance Windows and Customer Windows Tickets obtained from the Maintenance Windows System to determine whether: • Appropriate notifications were sent to customers if necessary • The query used to generate the listing contained the appropriate selection criteria
Results of Tests: No deviations noted.	

Common Criteria Related to Risk Management and Design and Implementation of Controls

CC3.1 The entity (1) identifies potential threats that could impair system security and availability commitments and system requirements (including threats arising from the use of vendors and other third parties providing goods and services, as well as threats arising from customer personnel and others with access to the system); (2) analyzes the significance of risks associated with the identified threats; (3) determines mitigation strategies for those risks (including implementation of controls, assessment and monitoring of vendors and other third parties providing goods or services, as well as their activities, and other mitigation strategies); (4) identifies and assesses changes (for example, environmental, regulatory, and technological changes and results of the assessment and monitoring of controls) that could significantly affect the system of internal control; and (5) reassesses, and revises as necessary, risk assessments and mitigation strategies based on the identified changes.	
Controls specified by ViaWest, Inc.	**Tests performed**
4.1: Network monitoring systems are used to monitor network events. These events are collected centrally and monitored by the Virtual Technical Assistance Center (VTAC) and/or DC Customer Support (DCCS) personnel. Monitoring systems are redundant to provide failover capability.	Inquired of the Senior Client Network Engineer to determine whether network monitoring tools were in place, redundant, and automatically report network incidents to management. Observed network monitoring tools to determine whether the tools were redundant and were monitoring network events. Inspected the network monitoring system configurations to determine whether the system was configured to monitor network devices. Obtained a population of network devices from the RANCID and Net Line Dancer tools. For a sample of network devices, inspected the configuration files on the device to determine whether: • The devices were configured to report events to the monitoring systems • The query used to generate the network device listing contained the appropriate selection criteria
SEC3.01A: On a monthly basis, the ViaWest Quality, Security and Compliance (QSC) Executive Governance Committee and QSC Management Governance Committee meet to identify potential threats to the system in the areas of security and availability based on information collected throughout the period from various sources throughout the organization.	Inspected the ViaWest Information Security Program document to determine whether governance committees have been established and consist of members of various departments throughout the organization. For a sample of months, obtained and inspected the QSC Executive Governance Committee and QSC Management Governance Committee meeting invitations to determine whether an appropriate cross-section of executive and management personnel were in attendance and inspected the meeting minutes to determine whether the meeting topics covered appropriate security and availability topics per the charter.

Common Criteria Related to Risk Management and Design and Implementation of Controls

CC3.1 The entity (1) identifies potential threats that could impair system security and availability commitments and system requirements (including threats arising from the use of vendors and other third parties providing goods and services, as well as threats arising from customer personnel and others with access to the system); (2) analyzes the significance of risks associated with the identified threats; (3) determines mitigation strategies for those risks (including implementation of controls, assessment and monitoring of vendors and other third parties providing goods or services, as well as their activities, and other mitigation strategies); (4) identifies and assesses changes (for example, environmental, regulatory, and technological changes and results of the assessment and monitoring of controls) that could significantly affect the system of internal control; and (5) reassesses, and revises, as necessary, risk assessments and mitigation strategies based on the identified changes. (continued)	
Controls specified by ViaWest, Inc.	**Tests performed**
SEC3.07A: Representatives from ViaWest Operations, Data Center Services, VTAC, Service Delivery, Managed Services, Network Engineering, Client Relationship Management, and Business Controls and Compliance groups meet weekly during the AARB meeting to evaluate, analyze, and define plans as necessary to discuss any issues that have disrupted service to customers. If a risk is identified, a project plan is created, resulting in changes.	For a sample of weeks, inspected calendar entries and meeting minutes to determine whether management scheduled and held the AARB meeting and representatives from the various groups were invited and attended. Inspected the AARB Tracking document to determine whether management documented issues and resolutions within the document on an ongoing basis.
CC3.1B: Risks are collected, evaluated, prioritized, addressed and tracked in JIRA.	Inspected a sample JIRA entry and determined that it contained information related to risks identified by management, an analysis of the risk, and the status of addressing the risk. For a sample of weeks, inspected the meeting invites for the Weekly Ambassador meetings to determine that risks were discussed as part of the agenda.
Results of Tests: No deviations noted.	

Common Criteria Related to Risk Management and Design and Implementation of Controls

CC3.2 The entity designs, develops, implements, and operates controls, including policies and procedures, to implement its risk mitigation strategy; reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities; and updates the controls, as necessary.	
Controls specified by ViaWest, Inc.	**Tests performed**
SEC1.01A: ViaWest policies and procedures are established, and responsibility for the policies and procedures is defined and assigned to specific policy owners, the CSO and compliance.	Inquired of the Director of Compliance to determine whether responsibility for the maintenance of ViaWest policies and procedures was established and defined. Inspected policy and procedure documents to determine whether they existed and provided guidance for employees in managing the activities of the business.
SEC1.01B: ViaWest policy and procedure documents are reviewed and updated by assigned parties and policy owners as needed. Updates to the policies are noted within the policy. An update date and reviewer/approver are identified within the policies and procedures.	Inquired of the Director of Compliance to determine whether responsibility for the maintenance of ViaWest policies and procedures was established and defined. Inspected a sample of policy and procedure documents to determine whether assigned parties and policy owners for the selected policies and procedures reviewed and approved any updates to the documents.
CC3.1B: Risks are collected, evaluated, prioritized, addressed and tracked in JIRA.	Inspected a sample JIRA entry and determined that it contained information related to risks identified by management, an analysis of the risk, and the status of addressing the risk. For a sample of weeks, inspected the meeting invites for the Weekly Ambassador meetings to determine that risks were discussed as part of the agenda.
CC5.1A: Corporate Security Scans are performed monthly. The results are sent to the internal IT Team, which is responsible for investigation and remediation efforts. The Customer Support Portal is scanned each weekend. These results are sent to the Development Team for investigation and remediation.	Inspected a sample of monthly Nessus scans and Weekly WhiteHat scans to determine whether scanning was occurring. From a sample Nessus and WhiteHat scan, inspected the JIRA ticket details for a sample vulnerability identified by the scan to determine whether the issues identified were researched and action was taken if necessary.
CC1.2C: Responsibility for each system control has been assigned to a member of management. On an annual basis, the control owners review the control to determine whether it addresses the risks of the current system requirements.	Inspected the listing of controls in the master control matrix to determine whether each control was assigned a control owner. For a sample of controls, inspected job titles and email evidence to determine whether the owner was appropriate based on his/her job responsibilities, the owner reviewed and approved the current control, and any changes identified were subsequently identified and communicated.
Results of Tests: No deviations noted.	

Common Criteria Related to Monitoring of Controls

CC4.1 The design and operating effectiveness of controls are periodically evaluated against the entity's commitments and system requirements as they relate to security and availability, and corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.	
Controls specified by ViaWest, Inc.	**Tests performed**
4.1: Network monitoring systems are used to monitor network events. These events are collected centrally and monitored by the Virtual Technical Assistance Center (VTAC) and/or DCCS personnel. Monitoring systems are redundant to provide failover capability.	Inquired of the Senior Client Network Engineer to determine whether network monitoring tools were in place, redundant, and automatically report network incidents to management. Observed network monitoring tools to determine whether the tools were redundant and were monitoring network events. Inspected the network monitoring system configurations to determine whether the system was configured to monitor network devices. Obtained a population of network devices from the RANCID and Net Line Dancer tools. For a sample of network devices, inspected the configuration files on the device to determine whether: • The devices were configured to report events to the monitoring systems • The query used to generate the network device listing contained the appropriate selection criteria
4.5: Data centers are monitored by VTAC and DCCS personnel who provide customer support, remote hands and monitoring of network events 24 hours a day, 7 days a week.	Inquired of the Data Center Managers to determine whether each data center location was monitored 24 hours a day, 7 days a week. Inspected DCCS personnel schedules to determine whether staff was scheduled to monitor each data center 24 hours a day, 7 days a week. For a sample of the in-scope data centers, observed monitoring systems in use at each data center to determine whether they were available. For a sample of the in-scope data centers, observed DCCS and/or VTAC personnel monitoring the status of the backbone and network events.
SEC3.07A: Representatives from ViaWest Operations, Data Center Services, VTAC, Service Delivery, Managed Services, Network Engineering, Client Relationship Management, and Business Controls and Compliance groups meet weekly during the AARB meeting to evaluate, analyze, and define plans as necessary to discuss any issues that have disrupted service to customers. If a risk is identified, a project plan is created, resulting in changes.	For a sample of weeks, inspected calendar entries and meeting minutes to determine whether management scheduled and held the AARB meeting and representatives from the various groups were invited and attended. Inspected the AARB Tracking document to determine whether management documented issues and resolutions within the document on an ongoing basis.

Common Criteria Related to Monitoring of Controls

CC4.1 The design and operating effectiveness of controls are periodically evaluated against the entity's commitments and system requirements as they relate to security and availability, and corrections and other necessary actions relating to identified deficiencies are taken in a timely manner. (continued)	
Controls specified by ViaWest, Inc.	**Tests performed**
SEC4.01A: ViaWest uses third-party tools to periodically assess new system security and engages third parties periodically to perform industry-required security assessments. High-risk issues are remediated.	Inspected third-party assessment reports to determine whether ViaWest engaged a third party to assess its system and, for high-risk issues noted, inspected the assessment reports or internal ViaWest documentation to determine whether high-risk issues were remediated.
4.6: On a monthly basis, management meets to review network, power, and physical space capacity for the data centers.	Observed a monthly Capacity Planning meeting and determined that each data center/region was discussed and evaluated based on remaining capacity of physical space and critical infrastructure, including cooling, backup power, and utilities using current capacity as well as sales projections. Inspected a sample of monthly capacity reports from the various building management, network, and data center systems and meeting agendas to determine whether monthly management meetings were held and reports were distributed and discussed.
Results of Tests: No deviations noted.	

Common Criteria Related to Logical and Physical Access Controls

CC5.1 Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to security and availability.	
Controls specified by ViaWest, Inc.	**Tests performed**
1.1: Administrative access to ViaWest support systems, applications, and network devices is limited to authorized personnel.	Obtained system-generated access listings from the ACS network device authentication tool and the associated queries used to generate the listings and inspected the user accounts with administrator access to determine whether: • Administrative access to the network devices via the ACS authentication tool was limited to authorized personnel based on inquiry with the Director of Network Services and inspection of the account owner's job function • The queries used to generate the listings contained the appropriate selection criteria Identified the population of Colocation and Managed Services network devices in the RANCID system and the query used to generate the population. For a sample of network devices, inspected IP addresses with permitted access to the devices to determine whether: • Defined IP addresses were limited to ViaWest internal IP addresses • The query used to generate the network device listing contained the appropriate selection criteria Obtained system-generated access listings from the ViaWest corporate domain and the associated query used to generate the listing and inspected the user accounts with administrator access to determine whether: • Administrative access to the ViaWest domain was limited to authorized personnel based on inquiry with the Director of Network Services and inspection of the account owners' job function • The query used to generate the listing contained the appropriate selection criteria

Common Criteria Related to Logical and Physical Access Controls

CC5.1 Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to security and availability. (continued)	
Controls specified by ViaWest, Inc.	**Tests performed**
1.1: Administrative access to ViaWest support systems, applications, and network devices is limited to authorized personnel. (continued)	Obtained the system-generated access listing from the Nimbus application, observed how the listing was generated, and inspected the user accounts to determine whether: • Administrative access to Nimbus was limited to authorized personnel based on inquiry with the Director of Network Services and inspection of the account owners' job function • The query used to generate the listing contained the appropriate selection criteria
6.1: Administrative access to ViaWest support systems, applications and devices supporting the Managed Services and Client Center Cloud environments is limited to authorized personnel.	Obtained system-generated access listings from the ACS network device authentication tool and the associated queries used to generate the listings and inspected the user accounts with administrator access to determine whether: • Administrative access to the network devices via the ACS authentication tool was limited to authorized personnel based on inquiry with the Director of Network Services and inspection of the account owner's job function • The queries used to generate the listings contained the appropriate selection criteria Obtained system-generated report of Colocation, Managed Services, and Client Center Cloud network devices and the associated query used to generate the listing and, for a sample of network devices, inspected IP addresses with permitted access to the devices to determine whether: • Defined IP addresses were limited to ViaWest internal IP addresses • The query used to generate the network device listing contained the appropriate selection criteria

Common Criteria Related to Logical and Physical Access Controls

CC5.1 Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to security and availability. (continued)	
Controls specified by ViaWest, Inc.	**Tests performed**
6.1: Administrative access to ViaWest support systems, applications and devices supporting the Managed Services and Client Center Cloud environments is limited to authorized personnel. (continued)	Obtained system-generated access listings from the Managed Services domain and the associated query used to generate the listing and inspected the user accounts with administrator access to determine whether: • Administrative access to the Managed Services domain was limited to authorized personnel based on inquiry with the Director of Network Services and inspection of the account owner's job function • The query used to generate the listing contained the appropriate selection criteria Obtained system-generated access listings from the Client Center Cloud domains and the associated queries used to generate the listings and inspected the user accounts with administrator access to determine whether: • Administrative access to the Client Center Cloud domains was limited to authorized personnel based on inquiry with the Ops Engineering Manager and inspection of the account owner's job function • The query used to generate the listing contained the appropriate selection criteria Obtained system-generated access listings from the Puppet tool used for the Client Center Cloud and the associated query used to generate the listing and inspected the user accounts with administrator access to determine whether: • Administrative access to the Puppet tool was limited to authorized personnel based on inquiry with the Ops Engineering Manager and inspection of the account owner's job function • The query used to generate the listing contained the appropriate selection criteria

Common Criteria Related to Logical and Physical Access Controls

CC5.1 Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to security and availability. (continued)	
Controls specified by ViaWest, Inc.	**Tests performed**
6.1: Administrative access to ViaWest support systems, applications and devices supporting the Managed Services and Client Center Cloud environments is limited to authorized personnel. (continued)	Obtained system-generated access listings from the Net Line Dancer tool used for the Client Center Cloud and the associated query used to generate the listing and inspected the user accounts with administrator access to determine whether: • Administrative access to the Net Line Dancer tool was limited to authorized personnel based on inquiry with the Network Engineer and inspection of the account owner's job function • The query used to generate the listing contained the appropriate selection criteria
1.2: Strong password settings, including minimum length, complexity requirements, password expiration, and password history, are configured and in place to restrict access to systems, network devices, and applications.	Inspected Cadence and Maintenance Window code to determine whether Cadence was configured to authenticate users through the ViaWest Global Directory Service password. Inspected Active Directory password security configurations on the corporate domain to determine whether password settings were set in conformance with ViaWest security policies. Inspected configurations within the ACS tool to determine whether authentication to TACACS and Radius required two factor authentication. Identified the population of Colocation and Managed Services network devices in the RANCID system and the query used to generate the population and, for a sample of network devices, inspected device configuration files to determine whether: • The network device was appropriately configured to require TACACS or Radius authentication • The query used to generate the network device listing contained the appropriate selection criteria Inspected configurations within the Nimbus application to determine whether it was configured to authenticate users to the system through the Active Directory password policy.

Common Criteria Related to Logical and Physical Access Controls

CC5.1 Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to security and availability. (continued)	
Controls specified by ViaWest, Inc.	**Tests performed**
6.2: Strong password settings, including minimum length, complexity requirements, password expiration and password history, are configured and in place to restrict access to systems, network devices and applications that support the Managed Services environment.	Inspected Customer Portal code to determine whether the Customer Portal was configured to authenticate users through Active Directory passwords. Inspected ACS configurations to determine whether Radius was configured to authenticate users to the system through Active Directory passwords. Inspected the Managed Services Active Directory password security configurations to determine whether password settings were in conformance with ViaWest security policies. Identified the population of Colocation and Managed Services network devices in the RANCID system and the query used to generate the population and, for a sample of network devices, inspected device configuration files to determine whether: • The network device was appropriately configured to require TACACS or Radius authentication • The query used to generate the network device listing contained the appropriate selection criteria Inspected Client Center Portal code to determine whether the Customer Portal was configured to authenticate users through Active Directory passwords. Inspected the Client Center Cloud corporate domain Active Directory password security configurations to determine whether password settings were in conformance with ViaWest security policies. Inspected the Client Center Cloud client domain Active Directory password security configurations to determine whether password settings were in conformance with ViaWest security policies. Inspected Puppet code to determine whether the Puppet was configured to authenticate users through Active Directory passwords. Inspected Conflux code to determine whether password settings were in conformance with ViaWest password policies.

Common Criteria Related to Logical and Physical Access Controls

CC5.1 Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to security and availability. (continued)

Controls specified by ViaWest, Inc.	Tests performed
6.2: Strong password settings, including minimum length, complexity requirements, password expiration and password history, are configured and in place to restrict access to systems, network devices and applications that support the Managed Services environment. (continued)	Inspected Cerberus code to determine whether Cerberus was configured to authenticate users through Active Directory passwords. Inspected Nagios code to determine whether Nagios was configured to authenticate users through Active Directory passwords. Inspected Net Line Dancer code to determine whether password settings were in conformance with ViaWest password policies.
CC5.1A: Corporate Security Scans are performed monthly. The results are sent to the internal IT Team, which is responsible for investigation and remediation efforts. The Customer Support Portal is scanned each weekend. These results are sent to the Development Team for investigation and remediation.	Inspected a sample of monthly Nessus scans and Weekly WhiteHat scans to determine whether scanning was occurring. From a sample Nessus and WhiteHat scan, inspected the JIRA ticket details for a sample vulnerability identified by the scan to determine whether the issues identified were researched and action was taken if necessary.

Results of Test: Of a sample of 100% of users with administrative access to the Puppet application, one terminated employee retained access. EY inspected evidence that the Active Directory account had been disabled in a timely manner after the employee's termination so that the user could not access the application. We also inspected evidence that the user's account had been disabled as of October 17, 2017.

Management Response: The user did not have the ability to log into the Puppet application after termination, as the user's network account had been disabled in a timely manner.

Results of Test: The Net Line Dancer application was not configured to require users to create passwords in conformance with the ViaWest Password Policy. Per inquiry with the Net Line Dancer Application Administrator, a complex random password is generated for each new user at the time the user is provisioned, and the system does not force the new user to change the random password. Per inquiry of a sample of Net Line Dancer users, they had implemented a strong password for their user account, in conformance with the ViaWest Password Policy.

Management Response: The Net Line Dancer application has been configured to authenticate using Client Center Cloud Active Directory Credentials as of October 20, 2017.

Common Criteria Related to Logical and Physical Access Controls

CC5.2 New internal and external users, whose access is administered by the entity, are registered and authorized prior to being issued system credentials and granted the ability to access the system to meet the entity's commitments and system requirements as they relate to security and availability. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	
Controls specified by ViaWest, Inc.	**Tests performed**
1.3: New or modified access to ViaWest systems is authorized by an appropriate manager.	Obtained system-generated access listings of relevant TACACS and Radius Active Directory groups and compared to system-generated listings of users from the prior period to identify a sample of new users with access to the network devices. Inspected the associated query used to generate the listings and inspected approval evidence for a sample of new or modified users to determine whether: • The appropriate manager approval for access was obtained and verified prior to allowing the user access to the network devices via TACACS authentication • The query used to generate the listing contained the appropriate selection criteria
6.3: New access to the Managed Services and Client Center Cloud client domain is authorized by an appropriate manager.	Obtained system-generated access listings from the Managed Services and Client Center Cloud client domains and the associated queries used to generate the listings and inspected approval evidence for a random sample of new users to determine whether: • The appropriate approval for requested access was obtained prior to allowing the user access to the domain • The query used to generate the listing contained the appropriate selection criteria
1.4: Names of terminated employees are communicated by Human Resources (HR) to management via email and/or the Cadence ticketing system. Management disables terminated employees from the ViaWest applications and network systems upon receipt of this notification.	For a sample of terminated employees from the termination listing from UltiPro, inspected the current TACACS and Radius user access listings, the current corporate domain user access listing, and emails from HR to determine whether: • HR notified IT of the employee's termination in a timely manner • Access was removed after the terminated user's termination date • The queries and parameters used to generate the listings contained the appropriate selection criteria

Common Criteria Related to Logical and Physical Access Controls

CC5.2 New internal and external users, whose access is administered by the entity, are registered and authorized prior to being issued system credentials and granted the ability to access the system to meet the entity's commitments and system requirements as they relate to security and availability. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized. (continued)	
Controls specified by ViaWest, Inc.	**Tests performed**
6.4: Terminated employees are communicated by Human Resources to management via email and/or the Cadence ticketing system. Management disables terminated employees from the ViaWest applications and network systems upon receipt of this notification.	Obtained the current ViaWest termination listing from HR, Managed Services domain user access listing, Client Center Cloud domain user access listing, the Customer Portal access listing, and the associated queries used to generate the listings and inspected all terminated employee's access to determine whether: • HR notified IT of the employee's termination in a timely manner • Access was removed after the terminated user's termination date • The queries and parameters used to generate the listings contained the appropriate selection criteria
1.5: Management performs semiannual user reviews on the badge systems and key applications and network devices to validate that user's access is commensurate with the individual's job function. If issues are identified, appropriate action is taken.	Obtained a sample of documentation for semiannual review procedures of user access to the network devices and administrator access to the badge systems performed by management and the associated queries used to generate the listings used in the reviews and inspected the documentation to determine whether: • Access was reviewed by the Director of Compliance and changes were made in accordance with the reviews • The queries used to generate the listings from the systems contained the appropriate selection criteria
6.5: Management performs user reviews on the Managed Services and Client Center Cloud tools and resources that grant access to client environments to validate that user's access is commensurate with the individual's job function. If issues are identified, appropriate action is taken.	Inspected documentation for a sample of semiannual reviews on the Managed Services domain, Cadence, and Radius to determine whether: • Access was reviewed by management in a timely manner and the review was performed with sufficient precision • Changes were made in accordance with the reviews • The queries used to generate the listings from the system contained the appropriate selection criteria Inspected documentation for a sample of quarterly reviews on the Client Center Cloud Windows and Linux Administrators groups to determine whether: • Access was reviewed by management in a timely manner and the review was performed with sufficient precision • Changes were made in accordance with the reviews • The queries used to generate the listings from the system contained the appropriate selection criteria

Common Criteria Related to Logical and Physical Access Controls

CC5.2 New internal and external users, whose access is administered by the entity, are registered and authorized prior to being issued system credentials and granted the ability to access the system to meet the entity's commitments and system requirements as they relate to security and availability. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized. (continued)
Results of Tests: For one of six new users tested that were granted access to the Managed Services network devices, the new user's request was documented in a ticket but was not approved by a manager prior to provisioning. ***Management Response:*** Based on the user's job function, and based on inquiry with the user's manager, the Director of Compliance, the Senior Windows Engineer, and the Director of Service Operations, the user's access was appropriate to be provisioned. ***Results of Test:*** Per inspection of the first semiannual review of users with administrative access to the badging systems, the review was not performed within one month of the end of the first half of the period. Furthermore, the review did not include evidence of secondary review by a user who did not have administrative access to the badging systems. Additionally, the review only included the two main badging systems and omitted two of the badging systems currently in use at certain data centers. EY tested the second semiannual review of users with administrative access to the badging systems and noted no further issues. ***Management Response:*** Although the review was not performed in a timely manner and did not include all four unique badging systems, the review was eventually performed within the examination period for all four systems. Furthermore, the initial review covered the systems that contained the majority of data centers within the Colocation System. Additionally, the required secondary review by a user who did not have administrative access to the system was performed, but was not documented. When this secondary review was performed, the reviewer agreed with the conclusions of the initial reviewer. Going forward, the company will maintain documented evidence of a secondary review. ***Results of Test:*** Per inspection of the first semiannual review of users with administrative access to the network devices, one user with privileged access was not included in the review. EY tested the second semiannual review of users with administrative access to the network devices and noted no further issues. ***Management Response:*** The user who was not reviewed belonged to a user group that was mistakenly omitted from the review. There was only one user within this group. This user has been determined to be appropriate to have administrative access to the network devices, such that no further action was needed. Going forward, this user group will be included in the review. ***Results of Test:*** The Windows group that grants administrative access to client Windows servers was not reviewed during the quarterly user access reviews for the Client Center Cloud. ***Management Response:*** A user access review was performed in October 2017, and no instances of inappropriate user access were identified.

Common Criteria Related to Logical and Physical Access Controls

CC5.3 Internal and external users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data) to meet the entity's commitments and system requirements as they relate to security and availability.	
Controls specified by ViaWest, Inc.	**Tests performed**
1.2: Strong password settings, including minimum length, complexity requirements, password expiration, and password history, are configured and in place to restrict access to systems, network devices, and applications.	Inspected Cadence and Maintenance Window code to determine whether Cadence was configured to authenticate users through the ViaWest Global Directory Service password. Inspected Active Directory password security configurations on the corporate domain to determine whether password settings were set in conformance with ViaWest security policies. Inspected configurations within the ACS tool to determine whether authentication to TACACS and Radius required two-factor authentication. Identified the population of Colocation and Managed Services network devices in the RANCID system and the query used to generate the population and, for a sample of network devices, inspected device configuration files to determine whether: • The network device was appropriately configured to require TACACS or Radius authentication • The query used to generate the network device listing contained the appropriate selection criteria Inspected configurations within the Nimbus application to determine whether it was configured to authenticate users to the system through the Active Directory password policy.
6.2: Strong password settings, including minimum length, complexity requirements, password expiration and password history, are configured and in place to restrict access to systems, network devices and applications that support the Managed Services environment.	Inspected Customer Portal code to determine whether the Customer Portal was configured to authenticate users through Active Directory passwords. Inspected ACS configurations to determine whether Radius was configured to authenticate users to the system through Active Directory passwords. Inspected the Managed Services Active Directory password security configurations to determine whether password settings were in conformance with ViaWest security policies.

Common Criteria Related to Logical and Physical Access Controls

CC5.3 Internal and external users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data) to meet the entity's commitments and system requirements as they relate to security and availability. (continued)	
Controls specified by ViaWest, Inc.	**Tests performed**
6.2: Strong password settings, including minimum length, complexity requirements, password expiration and password history, are configured and in place to restrict access to systems, network devices and applications that support the Managed Services environment. (continued)	Identified the population of Colocation and Managed Services network devices in the RANCID system and the query used to generate the population and, for a sample of network devices, inspected device configuration files to determine whether: • The network device was appropriately configured to require TACACS or Radius authentication • The query used to generate the network device listing contained the appropriate selection criteria Inspected Client Center Portal code to determine whether the Customer Portal was configured to authenticate users through Active Directory passwords. Inspected the Client Center Cloud corporate domain Active Directory password security configurations to determine whether password settings were in conformance with ViaWest security policies. Inspected the Client Center Cloud client domain Active Directory password security configurations to determine whether password settings were in conformance with ViaWest security policies. Inspected Puppet code to determine whether the Puppet was configured to authenticate users through Active Directory passwords. Inspected Conflux code to determine whether password settings were in conformance with ViaWest password policies. Inspected Cerberus code to determine whether the Cerberus was configured to authenticate users through Active Directory passwords. Inspected Nagios code to determine whether Nagios was configured to authenticate users through Active Directory passwords. Inspected Net Line Dancer code to determine whether password settings were in conformance with ViaWest password policies.
Results of Tests: The Net Line Dancer application was not configured to require users to create passwords in conformance with the ViaWest Password Policy. Per inquiry with the Net Line Dancer Application Administrator, a complex random password is generated for each new user at the time the user is provisioned, and the system does not force the new user to change the random password. Per inquiry of a sample of Net Line Dancer users, they had implemented a strong password for their user account, in conformance with the ViaWest Password Policy. ***Management Response:*** The Net Line Dancer application has been configured to authenticate using Client Center Cloud Active Directory credentials as of October 20, 2017.	

Common Criteria Related to Logical and Physical Access Controls

CC5.4 Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to meet the entity's commitments and system requirements as they relate to security and availability.	
Controls specified by ViaWest, Inc.	**Tests performed**
1.3: New or modified access to ViaWest systems is authorized by an appropriate manager.	Obtained system-generated access listings from the TACACS server and the associated query used to generate the listing and inspected approval evidence for a sample of new or modified users to determine whether: • The appropriate manager approval for access was obtained and verified prior to allowing the user access to the network devices via TACACS server authentication • The query used to generate the listing contained the appropriate selection criteria
6.3: New access to the Managed Services and Client Center Cloud client domain is authorized by an appropriate manager.	Obtained system-generated access listings from the Managed Services and Client Center Cloud client domains and the associated queries used to generate the listings and inspected approval evidence for a random sample of new users to determine whether: • The appropriate approval for requested access was obtained prior to allowing the user access to the domain. • The query used to generate the listing contained the appropriate selection criteria.
1.4: Names of terminated employees are communicated by Human Resources (HR) to management via email notifications and/or the Cadence ticketing system. Management disables terminated employees from the ViaWest applications and network systems upon receipt of this notification.	For a sample of terminated employees from the termination listing from UltiPro, inspected the current TACACS and Radius user access listings, the current corporate domain user access listing, and emails from HR to determine whether: • HR notified IT of the employee's termination in a timely manner • Access was removed after the terminated user's termination date • The queries and parameters used to generate the listings contained the appropriate selection criteria

Common Criteria Related to Logical and Physical Access Controls

CC5.4 Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to meet the entity's commitments and system requirements as they relate to security and availability. (continued)	
Controls specified by ViaWest, Inc.	**Tests performed**
6.4: Terminated employees are communicated by Human Resources to management via email and/or the Cadence ticketing system. Management disables terminated employees from the ViaWest applications and network systems upon receipt of this notification.	Obtained the current ViaWest termination listing from HR, the current Managed Services domain user access listing, the current Client Center Cloud domain user access listing, the Customer Portal access listing, and the associated queries used to generate the listings and inspected all terminated employee's access to determine whether: • HR notified IT of the employee's termination in a timely manner • Access was removed after the terminated user's termination date • The queries and parameters used to generate the listings contained the appropriate selection criteria
1.5: Management performs semiannual user reviews on the badge systems and key applications and network devices to validate that user's access is commensurate with the individual's job function. If issues are identified, appropriate action is taken.	Obtained a sample of documentation for semiannual review procedures of user access to the network devices and administrator access to the badge systems performed by management and the associated queries used to generate the listings used in the reviews and inspected the documentation to determine whether: • Access was reviewed by the Director of Compliance and changes were made in accordance with the reviews • The queries used to generate the listings from the systems contained the appropriate selection criteria
6.5: Management performs user reviews on the Managed Services and Client Center Cloud tools and resources that grant access to client environments to validate that user's access is commensurate with the individual's job function. If issues are identified, appropriate action is taken.	Inspected documentation for a sample of semiannual reviews on the Managed Services domain, Cadence, and Radius to determine whether: • Access was reviewed by management in a timely manner and the review was performed with sufficient precision • Changes were made in accordance with the reviews • The queries used to generate the listings from the system contained the appropriate selection criteria

Common Criteria Related to Logical and Physical Access Controls

CC5.4 Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to meet the entity's commitments and system requirements as they relate to security and availability. (continued)	
Controls specified by ViaWest, Inc.	**Tests performed**
6.5: Management performs user reviews on the Managed Services and Client Center Cloud tools and resources that grant access to client environments to validate that user's access is commensurate with the individual's job function. If issues are identified, appropriate action is taken. (continued)	Inspected documentation for a sample of quarterly reviews on the Client Center Cloud Windows and Linux Administrators groups to determine whether: • Access was reviewed by management in a timely manner and the review was performed with sufficient precision • Changes were made in accordance with the reviews • The queries used to generate the listings from the system contained the appropriate selection criteria
Results of Test: For one of six new users tested that were granted access to the Managed Services network devices, the new user's request was documented in a ticket but was not approved by a manager prior to provisioning. ***Management Response:*** Based on the user's job function and based on inquiry with the user's manager, the Director of Compliance, the Senior Windows Engineer, and the Director of Service Operations, the user's access was appropriate to be provisioned. ***Results of Test:*** Per inspection of the first semiannual review of users with administrative access to the badging systems, the review was not performed within one month of the end of the first half of the period. Further, the review did not include evidence of secondary review by a user who did not have administrative access to the badging systems. Additionally, the review performed only included the two main badging systems and omitted two of the badging systems currently in use at certain data centers. EY tested the second semiannual review of users with administrative access to the badging systems and noted no further issues. ***Management Response:*** Although the review was not performed in a timely manner and did not include all four unique badging systems, the review was eventually performed within the examination period for all four systems. Furthermore, the initial review covered the systems that contained the majority of data centers within the Colocation System. Additionally, the required secondary review by a user who did not have administrative access to the system was performed but was not documented. When this secondary review was performed, the reviewer agreed with the conclusions of the initial reviewer. Going forward, the company will maintain documented evidence of a secondary review. ***Results of Test:*** Per inspection of the first semiannual review of users with administrative access to the network devices, one user with privileged access was not included in the review. EY tested the second semiannual review of users with administrative access to the network devices and noted no further issues. ***Management Response:*** The user who was not reviewed belonged to a user group that was mistakenly omitted from the review. There was only one user within this group. This user has been determined to be appropriate to have administrative access to the network devices, such that no further action was needed. Going forward, this user group will be included in the review. ***Results of Test:*** The Windows group that grants administrative access to client Windows servers was not reviewed during the quarterly user access reviews for the Client Center Cloud. ***Management Response:*** A user access review was performed in October 2017, and no instances of inappropriate user access were identified.	

Common Criteria Related to Logical and Physical Access Controls

CC5.5 Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations as well as sensitive system components within those locations) is restricted to authorized personnel to meet the entity's commitments and system requirements as they relate to security and availability.	
Controls specified by ViaWest, Inc.	**Tests performed**
2.1: New access to data centers, raised floor areas, and customer cages is approved by appropriate management personnel and designated customer personnel as appropriate.	Obtained the sample of new hires from the UltiPro new hire listing and the associated query used to generate the listing, and inspected badge access listings from each data center to determine whether the new hire was granted data center access and, for a sample of new hires granted center access, inspected the EPACA form to determine whether: • Access to the data centers was approved • The query used to generate the listings from the systems contained the appropriate selection criteria Obtained the population of new customer and vendor badge access by comparing badge access listings for each data center from prior year and current year listings, and the associated query used to generate the listings, selected a sample of new customers and vendors, and inspected approval documentation to determine whether: • The customer was authorized for data center access on the MySupport Portal or the vendor was authorized by the vendor single point of contact on the Vendor Access List form and a member of ViaWest data center management completed and approved the Access Card Receipt Acknowledgement form. • The queries used to generate the listings from the systems contained the appropriate selection criteria
2.2: Names of terminated employees are communicated by HR to management via email and/or the Cadence ticketing system. Upon termination notification, physical access to the data center is removed.	Obtained the current ViaWest termination listing from UltiPro, the current badge access listings for all in-scope data centers, and the associated queries used to generate the listings and, for a sample of terminated users, inspected the badge access listings for all in-scope data centers to determine whether: • The individual's physical access was removed from all data center locations upon termination • The queries used to generate the listings from the system contained the appropriate selection criteria

Common Criteria Related to Logical and Physical Access Controls

CC5.5 Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations as well as sensitive system components within those locations) is restricted to authorized personnel to meet the entity's commitments and system requirements as they relate to security and availability. (continued)	
Controls specified by ViaWest, Inc.	**Tests performed**
2.3: Physical access to ViaWest data centers for employees, vendors, and customers is inspected by ViaWest management on a quarterly basis to confirm that access is authorized. Any issues noted are resolved by ViaWest management.	Inspected documentation for a sample of quarterly physical access reviews performed by Physical Security and the completeness and accuracy procedures performed by management to generate the user listings to determine whether: • The DCCS Supervisor completed and approved the review • For a sample of noted changes, the selected changes were resolved • The data used in the review was sufficiently detailed to detect inappropriate access to the data centers • The queries used to generate the listings from the system contained the appropriate selection criteria Inquired of the personnel performing the review to determine whether the reviewer had sufficient knowledge of the listings and subject matter and whether the level of detail inspected by the reviewer was sufficient to detect inappropriate access to the data centers.
2.4: Physical access mechanisms (e.g., access badge, biometric devices) have been implemented and are administered to help confirm that only authorized individuals have the ability to access the ViaWest data centers.	For the data centers physically visited during the examination period, observed that the exterior doors of the data center required a badge for entry. For the data centers physically visited during the examination period, observed that in order to access the raised floor area or Network Operations Centers, either a PIN or biometric hand/finger scan was required before entry.
2.5: Internal and external physical monitoring of data center activity is performed through the use of ViaWest DCCS personnel, data center walk-throughs, alarms, and security cameras.	For the data centers physically visited during the examination period, observed DCCS staff monitoring the security cameras and alarm systems and performing periodic walk-throughs. For the data centers physically visited during the examination period, observed security cameras and other physical access monitoring tools throughout the facility. Inquired of the Senior Data Center Manager to determine whether DCCS staff performed periodic walk-throughs of the data center facilities. For a sample of auto-generated data center walk-through tickets in Cadence, inspected ticket details to determine whether: • The data center walk-through was completed within eight hours • The query used to generate the population from the ticketing system contained the appropriate selection criteria

Common Criteria Related to Logical and Physical Access Controls

CC5.5 Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations as well as sensitive system components within those locations) is restricted to authorized personnel to meet the entity's commitments and system requirements as they relate to security and availability. (continued)	
Controls specified by ViaWest, Inc.	**Tests performed**
2.6: Customer-specific areas (including cabinets, cages, and suites) are secured with additional security mechanisms, such as combination locks, keys, or biometric readers.	For the data centers physically visited during the examination period, observed whether customer-specific areas were secured with combination locks, keys, or biometric readers. For the data centers physically visited during the examination period, observed whether keys and master keys were secured.
2.7: Each customer has a defined space within the data center that is physically secured within a locked cage, cabinet, or suite.	For the data centers physically visited during the examination period, observed whether customers' equipment was secured in locked cages or cabinets.
2.8: ViaWest reviews access to the data centers operated by subservice organizations on an annual basis.	Obtained a sample of documentation for annual review procedures of user access to the Westin and Equinix data centers performed by management and the associated queries used to generate the listings used in the reviews and inspected the documentation to determine whether: • Access was reviewed by the Director of Compliance and changes were made in accordance with the reviews • The queries used to generate the listings from the systems contained the appropriate selection criteria
Results of Test: Two of 11 sampled new employees with data center access did not have a signed EPACA form prior to being granted access to the data center. EY inspected system logs showing that these users did not access the data center during the time that they had inappropriate access. EY inspected user access listings as of September 15, 2017, that demonstrate that the access had been subsequently removed. ***Management Response:*** The access for both users was removed, and employees have been retrained on the requirements for granting access to the data centers. ***Results of Test:*** One of five new customers and vendors sampled with data center access did not have a signed Customer or Vendor DC Access Card Receipt and Acknowledgement form. ***Management Response:*** The customer personnel was authorized to enter the data center per the MySupport Portal. However, since the customer personnel did not physically sign the form, the customer personnel's access was disabled as of October 17, 2017, and will remain disabled until the form is signed.	

Common Criteria Related to Logical and Physical Access Controls

CC5.6 Logical access security measures have been implemented to protect against security and availability threats from sources outside the boundaries of the system to meet the entity's commitments and system requirements.	
Controls specified by ViaWest, Inc.	**Tests performed**
6.6: Default policies on customer-specific firewalls are configured to restrict access to only ViaWest monitoring systems and appropriate Operations personnel.	Inspected the base configuration policy to determine whether the IP addresses permitted to the policy were restricted to appropriate ViaWest systems, servers, and personnel. Inspected the population of customer-specific firewall devices in the Managed Services environment from the RANCID application and the query used to generate the listing to determine whether the appropriate selection criteria was applied. Identified a sample of customer firewalls and, for a sample of customer-specific firewalls, inspected the policies to determine whether the standard base configuration was applied.
6.7: Policies added or modified on the customer-specific firewalls are authorized by the customer contract or subsequent modification request.	Inspected the population of customer-specific firewall devices in the Managed Services environment from the RANCID application and the query used to generate the listing to determine whether the appropriate selection criteria was applied. Selected a sample of customer firewalls and, for a sample custom policy on each firewall, inspected the customer contract or customer ticket to determine whether the policy was configured in accordance with a customer request.
SEC3.4A: ViaWest uses access control lists to prevent unauthorized access to the colocation network devices. Only authorized access points can access the ViaWest network devices.	Obtained system-generated report of Colocation and Managed Services network devices and the associated query used to generate the listing and, for a sample of network devices, inspected IP addresses with permitted access to the devices to determine whether: • Defined IP addresses were limited to ViaWest internal IP addresses • The query used to generate the network device listing contained the appropriate selection criteria
SEC4.01A: ViaWest uses third-party tools to periodically assess new system security and engages third parties periodically to perform industry-required security assessments. High-risk issues are remediated.	Inspected third-party assessment reports to determine whether ViaWest engaged a third party to assess its system and, for high-risk issues noted, inspected the assessment reports or internal ViaWest documentation to determine whether high-risk issues were remediated.
Results of Test: No deviations noted.	

Common Criteria Related to Logical and Physical Access Controls

CC5.7 The transmission, movement, and removal of information are restricted to authorized internal and external users and processes, and is protected during transmission, movement, or removal, enabling the entity to meet its commitments and system requirements as they relate to security and availability.	
Controls specified by ViaWest, Inc.	**Tests performed**
SEC3.06A: Access methods to network devices that support the collocation system are encrypted.	Inspected ACS tool, which authenticates users to network devices, and reviewed its security configuration to determine whether encryption techniques were employed to access network devices. Observed a ViaWest employee accessing a network device to determine whether the employee's access session was encrypted using an RSA token. Obtained system-generated report of colocation network devices and the associated query used to generate the listing and, for a sample of network devices, inspected device configurations to determine whether: • The network device was appropriately configured per ViaWest security configuration requirements • The query used to generate the network device listing contained the appropriate selection criteria. Observed one ViaWest employee accessing a network device within the Client Center Cloud environment to determine whether the employee's access session was encrypted using an RSA token.
Results of Test: No deviations noted.	

Common Criteria Related to Logical and Physical Access Controls

CC5.8 Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's commitments and system requirements as they relate to security and availability.	
Controls specified by ViaWest, Inc.	**Tests performed**
SEC3.05A: ViaWest servers and laptops are configured with antivirus software, which is updated by the vendor, and various scans are performed regularly.	Inspected a sample laptop and a sample server to determine whether antivirus software was enabled on the systems and configured to run periodic updates and scans. Inspected configurations on the tools used to manage antivirus policies for all laptops and servers to determine whether the tools were configured to scan laptops and servers within the network.
Results of Test: No deviations noted.	

Common Criteria Related to System Operations

CC6.1 Vulnerabilities of system components to security and availability breaches and incidents due to malicious acts, natural disasters, or errors are identified, monitored, and evaluated, and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities to meet the entity's commitments and system requirements as they relate to security and availability.	
Controls specified by ViaWest, Inc.	**Tests performed**
SEC3.07A: Representatives from ViaWest Operations, Data Center Services, VTAC, Service Delivery, Managed Services, Network Engineering, Client Relationship Management, and Business Controls and Compliance groups meet weekly during the AARB meeting to evaluate, analyze, and define plans as necessary to discuss any issues that have disrupted service to customers. If a risk is identified, a project plan is created, resulting in changes.	For a sample of weeks, inspected calendar entries and meeting minutes to determine whether management scheduled and held the AARB meeting and representatives from the various groups were invited and attended. Inspected the AARB tracking document to determine whether management documented issues and resolutions within the document on an ongoing basis.
CC5.1A: Corporate Security Scans are performed monthly. The results are sent to the internal IT Team, which is responsible for investigation and remediation efforts. The Customer Support Portal is scanned each weekend. These results are sent to the Development Team for investigation and remediation.	Inspected a sample of monthly Nessus scans and Weekly WhiteHat scans to determine whether scanning was occurring. From a sample Nessus and WhiteHat scan, inspected the JIRA ticket details for a sample vulnerability identified by the scan to determine whether the issues identified were researched and action was taken if necessary.
5.8: Critical network device configurations are backed up using RANCID and Net Line Dancer on a nightly basis.	Obtained a population of network devices from Rancid and Net Line Dancer and the queries used to generate the population. For a sample of network devices, inspected the log files on RANCID or Net Line Dancer to determine whether: • Net Line Dancer took a snapshot of configuration changes on the device from the previous day • The query used to generate the network device listing contained the appropriate selection criteria
5.9: Managed Services and Client Center Cloud servers are backed up on a daily basis. Alerts are configured to notify ViaWest personnel in the event of a backup failure.	Inquired of Backup Engineer to determine whether backups are performed on a regular basis by a backup tool. For a sample day, inspected the backup log for a sample Managed Services client server and a sample Client Center Cloud client server to determine that the backup was completed and replicated to an off-site server. For a sample Managed Services and a sample Client Center Cloud client server, inspected the backup tool to confirm alerts related to failed backups are configured to be sent to client personnel. For a sample failed backup, inspected the Cadence ticket or Nagios alert to determine whether the backup tool automatically generated a ticket and whether the ticket was resolved in a timely manner.
Results of Test: No deviations noted.	

Common Criteria Related to System Operations

CC6.2 Security and availability incidents, including logical and physical security breaches, failures, and identified vulnerabilities, are identified and reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's commitments and system requirements.	
Controls specified by ViaWest, Inc.	**Tests performed**
4.1: Network monitoring systems are used to monitor network events. These events are collected centrally and monitored by the VTAC and/or DCCS personnel. Monitoring systems are redundant to provide failover capability.	Inquired of the Senior Monitoring Administrator to determine whether network monitoring tools were in place and redundant and automatically report network incidents to management. Observed network monitoring tools to determine whether the tools were redundant and were monitoring network events. Inspected the network monitoring system configurations to determine whether the system was configured to monitor network devices. Obtained a population of network devices from the RANCID and Net Line Dancer tools and, for a sample of network devices, inspected the configuration files on the device to determine whether: • The devices were configured to report events to the monitoring systems • The query used to generate the network device listing contained the appropriate selection criteria
4.2: Cadence and Cerberus tickets for customer impacting environmental, hardware and network changes, and network disruptions are tracked, prioritized, escalated, and assigned to resources based on documented policies and procedures. Customers are notified about unexpected events that may impact their systems.	Obtained the population of incidents from the Cadence ticketing system and the queries used to generate the population and, for a sample of Colocation and Managed Services tickets, inspected ticket details to determine whether: • The event was tracked, prioritized, escalated, and assigned to resources in accordance with documented policies and procedures and, if required, appropriate customer communications were made • The queries used to generate the listings from Cadence contained the appropriate selection criteria Inspected the application code for Cadence to determine whether Cadence created a ticket as priority "0" when a network monitoring system alarm was triggered by a device or network failure/issue. Inspected the alert configuration within Nagios to determine whether notifications are configured to be sent for Cerberus Site Down tickets that have not been responded to within the first minute. For a sample Site Down ticket, inspected an example email of the alert configuration to determine whether notifications were being sent to appropriate personnel.

Common Criteria Related to System Operations

CC6.2 Security and availability incidents, including logical and physical security breaches, failures, and identified vulnerabilities, are identified and reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's commitments and system requirements. (continued)	
Controls specified by ViaWest, Inc.	**Tests performed**
4.5: Data centers are monitored by VTAC and DCCS personnel who provide customer support, remote hands and monitoring of network events 24 hours a day, 7 days a week.	Inquired of the Data Center Managers to determine whether each data center location was monitored 24 hours a day, 7 days a week. Inspected DCCS personnel schedules to determine whether staff was scheduled to monitor each data center 24 hours a day, 7 days a week. For a sample of the in-scope data centers, observed monitoring systems in use at each data center to determine whether they were available. For a sample of the in-scope data centers, observed DCCS and/or VTAC personnel monitoring the status of the backbone and network events.
SEC3.07A: Representatives from ViaWest Operations, Data Center Services, VTAC, Service Delivery, Managed Services, Network Engineering, Client Relationship Management, and Business Controls and Compliance groups meet weekly during the AARB meeting to evaluate, analyze, and define plans as necessary to discuss any issues that have disrupted service to customers. If a risk is identified, a project plan is created, resulting in changes.	For a sample of weeks, inspected calendar entries and meeting minutes to determine whether management scheduled and held the AARB meeting and representatives from the various groups were invited and attended. Inspected the AARB tracking document to determine whether management documented issues and resolutions within the document on an ongoing basis.
CC5.1A: Corporate Security Scans are performed monthly. The results are sent to the internal IT Team, which is responsible for investigation and remediation efforts. The Customer Support Portal is scanned each weekend. These results are sent to the Development Team for investigation and remediation.	Inspected a sample of monthly Nessus scans and weekly WhiteHat scans to determine whether scanning was occurring. From a sample Nessus and WhiteHat scan, inspected the JIRA ticket details for a sample vulnerability identified by the scan to determine whether the issues identified were researched and action was taken if necessary.
Results of Test: For 5 of 26 incident tickets tested, the Cadence ticket was not prioritized within 5 minutes of the ticket creation. In each case, we inspected the ticket details and determined that the ticket was prioritized within 30 minutes. EY selected an additional 5 Cadence tickets and noted no further issues. ***Management Response:*** Although all tickets with an unassigned priority are acknowledged within the first few minutes of generation, during certain high-volume times the DCCS or VTAC personnel are not able to research the incident and conclude on a prioritization number within the first five minutes of the ticket being generated. Going forward, a practice of acknowledging the ticket receipt will be implemented if the ticket cannot be prioritized within the stated SLA.	

Common Criteria Related to Change Management

CC7.1 The entity's commitments and system requirements, as they relate to security and availability, are addressed during the system development life cycle, including the authorization, design, acquisition, implementation, configuration, testing, modification, approval, and maintenance of system components.	
Controls specified by ViaWest, Inc.	**Tests performed**
3.1: Non-routine modifications to network devices are made during Maintenance Windows authorized by management, and a back-out plan is documented for prior configuration recovery purposes.	Obtained the population of Maintenance Windows tickets and the associated query used to generate the listing and, for a sample of tickets, inspected ticket details and communication logs to determine whether: • The project plan and procedures to be performed were listed, the change was approved by an appropriate member of management and customers if necessary, and back-out procedures were documented • Appropriate notifications were sent to customers if necessary • The query used to generate the listing from the Maintenance Windows system contained the appropriate selection criteria
3.3: Network configuration changes are systematically logged within RANCID and Net Line Dancer and are captured for review.	For a haphazardly selected day, inspected a sample change notification to determine whether RANCID automatically generated the notification and forwarded to Network Operations for review. For a haphazardly selected day, inspected a sample change notification to determine whether Net Line Dancer automatically generated the notification and forwarded to a Network Engineer for a review. Obtained a population of network devices from RANCID and Net Line Dancer and the queries used to generate the population and, for a sample of network devices, inspected the log files on RANCID or Net Line Dancer to determine whether: • RANCID or Net Line Dancer took a snapshot of configuration changes on the device from the previous day • The query used to generate the network device listing contained the appropriate selection criteria Inspected the RANCID cron job to determine whether it was configured to run daily. Inspected the configuration of the daily change report on Net Line Dancer to determine whether it was configured to run daily.

Common Criteria Related to Change Management

CC7.1 The entity's commitments and system requirements, as they relate to security and availability, are addressed during the system development life cycle, including the authorization, design, acquisition, implementation, configuration, testing, modification, approval, and maintenance of system components. (continued)	
Controls specified by ViaWest, Inc.	**Tests performed**
3.3: Network configuration changes are systematically logged within RANCID and Net Line Dancer and are captured for review. (continued)	Inquired of the Senior Network Engineer to determine whether the daily emails containing the prior day's network configuration changes were monitored and reviewed. Inquired of the Senior Network Engineer to determine whether the daily emails containing the prior day's network configuration changes for the Client Center Cloud were monitored and reviewed.
CC7.1A: ViaWest has established policies and procedures related to change management, which govern the way that changes are initiated, tracked, tested, evaluated for security and availability considerations, and authorized for implementation.	Inspected the Change Management policies and procedures to determine whether criteria for system development have been established.
Results of Test: No deviations noted	

Common Criteria Related to Change Management

CC7.2 Infrastructure, data, software, and policies and procedures are updated as necessary to remain consistent with the entity's commitments and system commitments and requirements as they relate to security and availability.	
Controls specified by ViaWest, Inc.	**Tests performed**
3.1: Non-routine modifications to network devices are made during Maintenance Windows authorized by management, and a back-out plan is documented for prior configuration recovery purposes.	Obtained the population of Maintenance Windows tickets and the associated query used to generate the listing and, for a sample of tickets, inspected ticket details and communication logs to determine whether: • The project plan and procedures to be performed were listed, the change was approved by an appropriate member of management and customers if necessary, and back-out procedures were documented • Appropriate notifications were sent to customers if necessary • The query used to generate the listing from the Maintenance Windows system contained the appropriate selection criteria
3.3: Network configuration changes are systematically logged within RANCID and Net Line Dancer and are captured for review.	For a haphazardly selected day, inspected a sample change notification to determine whether RANCID automatically generated the notification and forwarded to Network Operations for review. For a haphazardly selected day, inspected a sample change notification to determine whether Net Line Dancer automatically generated the notification and forwarded to a Network Engineer for a review. Obtained a population of network devices from RANCID and Net Line Dancer and the queries used to generate the population and, for a sample of network devices, inspected the log files on RANCID or Net Line Dancer to determine whether: • RANCID or Net Line Dancer took a snapshot of configuration changes on the device from the previous day • The query used to generate the network device listing contained the appropriate selection criteria Inspected the RANCID cron job to determine whether it was configured to run daily. Inspected the configuration of the daily change report on Net Line Dancer to determine whether it was configured to run daily.

Common Criteria Related to Change Management

CC7.2 Infrastructure, data, software, and policies and procedures are updated as necessary to remain consistent with the entity's commitments and system commitments and requirements as they relate to security and availability. (continued)	
Controls specified by ViaWest, Inc.	**Tests performed**
3.3: Network configuration changes are systematically logged within RANCID and Net Line Dancer and are captured for review. (continued)	Inquired of the Senior Network Engineer to determine whether the daily emails containing the prior day's network configuration changes were monitored and reviewed. Inquired of the Senior Network Engineer to determine whether the daily emails containing the prior day's network configuration changes for the Client Center Cloud were monitored and reviewed.
SEC4.01A: ViaWest uses third-party tools to periodically assess new system security and engages third parties periodically to perform industry-required security assessments. High-risk issues are remediated.	Inspected third-party assessment reports to determine whether ViaWest engaged a third party to assess its system and, for high-risk issues noted, inspected the assessment reports or internal ViaWest documentation to determine whether high-risk issues were remediated.
SEC1.01B: ViaWest policy and procedure documents are reviewed and updated by assigned parties and policy owners as needed.	Inquired of the Director of Compliance to determine whether management periodically reviewed and updated policy and procedure documents throughout the course of the examination period. Inspected a sample of policy and procedure documents to determine whether assigned parties and policy owners for the selected policies and procedures reviewed and approved any updates to the documents.
Results of Test: No deviations noted	

Common Criteria Related to Change Management

CC7.3 Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and are monitored to meet the entity's commitments and system requirements as they relate to security and availability.	
Controls specified by ViaWest, Inc.	**Tests performed**
3.1: Non-routine modifications to network devices are made during Maintenance Windows authorized by management, and a back-out plan is documented for prior configuration recovery purposes.	Obtained the population of Maintenance Windows tickets and the associated query used to generate the listing and, for a sample of tickets, inspected ticket details and communication logs to determine whether: • The project plan and procedures to be performed were listed, the change was approved by an appropriate member of management and customers if necessary, and back-out procedures were documented • Appropriate notifications were sent to customers if necessary • The query used to generate the listing from the Maintenance Windows system contained the appropriate selection criteria
3.3: Network configuration changes are systematically logged within RANCID and Net Line Dancer and are captured for review.	For a haphazardly selected day, inspected a sample change notification to determine whether RANCID automatically generated the notification and forwarded to Network Operations for review. For a haphazardly selected day, inspected a sample change notification to determine whether Net Line Dancer automatically generated the notification and forwarded to a Network Engineer for a review. Obtained a population of network devices from RANCID and Net Line Dancer and the queries used to generate the population and, for a sample of network devices, inspected the log files on RANCID or Net Line Dancer to determine whether: • RANCID or Net Line Dancer took a snapshot of configuration changes on the device from the previous day • The query used to generate the network device listing contained the appropriate selection criteria Inspected the RANCID cron job to determine whether it was configured to run daily. Inspected the configuration of the daily change report on Net Line Dancer to determine whether it was configured to run daily.

Common Criteria Related to Change Management

CC7.3 Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and are monitored to meet the entity's commitments and system requirements as they relate to security and availability. (continued)	
Controls specified by ViaWest, Inc.	**Tests performed**
3.3: Network configuration changes are systematically logged within RANCID and Net Line Dancer and are captured for review. (continued)	Inquired of the Senior Network Engineer to determine whether the daily emails containing the prior day's network configuration changes were monitored and reviewed. Inquired of the Senior Network Engineer to determine whether the daily emails containing the prior day's network configuration changes for the Client Center Cloud were monitored and reviewed.
SEC4.01A: ViaWest uses third-party tools to periodically assess new system security and engages third parties periodically to perform industry-required security assessments. High-risk issues are remediated.	Inspected third-party assessment reports to determine whether ViaWest engaged a third party to assess its system and, for high-risk issues noted, inspected the assessment reports or internal ViaWest documentation to determine whether high-risk issues were remediated.
SEC3.07A: Representatives from ViaWest Operations, Data Center Services, VTAC, Service Delivery, Managed Services, Network Engineering, Client Relationship Management, and Business Controls and Compliance groups meet weekly during the AARB meeting to evaluate, analyze, and define plans as necessary to discuss any issues that have disrupted service to customers. If a risk is identified, a project plan is created, resulting in changes.	For a sample of weeks, inspected calendar entries and meeting minutes to determine whether management scheduled and held the AARB meeting and representatives from the various groups were invited and attended. Inspected the AARB tracking document to determine whether management documented issues and resolutions within the document on an ongoing basis.
Results of Test: No deviations noted	

Common Criteria Related to Change Management

CC7.4 Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented to meet the entity's security and availability commitments and system requirements.	
Controls specified by ViaWest, Inc.	**Tests performed**
3.1: Non-routine modifications to network devices are made during Maintenance Windows authorized by management, and a back-out plan is documented for prior configuration recovery purposes.	Obtained the population of Maintenance Windows tickets and the associated query used to generate the listing and, for a sample of tickets, inspected ticket details and communication logs to determine whether: • The project plan and procedures to be performed were listed, the change was approved by an appropriate member of management and customers if necessary, and back-out procedures were documented • Appropriate notifications were sent to customers if necessary • The query used to generate the listing from the Maintenance Windows system contained the appropriate selection criteria
3.3: Network configuration changes are systematically logged within RANCID and Net Line Dancer and are captured for review.	For a haphazardly selected day, inspected a sample change notification to determine whether RANCID automatically generated the notification and forwarded to Network Operations for review. For a haphazardly selected day, inspected a sample change notification to determine whether Net Line Dancer automatically generated the notification and forwarded to a Network Engineer for a review. Obtained a population of network devices from RANCID and Net Line Dancer and the queries used to generate the population and, for a sample of network devices, inspected the log files on RANCID or Net Line Dancer to determine whether: • RANCID or Net Line Dancer took a snapshot of configuration changes on the device from the previous day • The query used to generate the network device listing contained the appropriate selection criteria Inspected the RANCID cron job to determine whether it was configured to run daily. Inspected the configuration of the daily change report on Net Line Dancer to determine whether it was configured to run daily.

Common Criteria Related to Change Management

CC7.4 Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented to meet the entity's security and availability commitments and system requirements. (continued)	
Controls specified by ViaWest, Inc.	**Tests performed**
3.3: Network configuration changes are systematically logged within RANCID and Net Line Dancer and are captured for review. (continued)	Inquired of the Senior Network Engineer to determine whether the daily emails containing the prior day's network configuration changes were monitored and reviewed. Inquired of the Senior Network Engineer to determine whether the daily emails containing the prior day's network configuration changes for the Client Center Cloud were monitored and reviewed.
Results of Test: No deviations noted	

Additional Criteria for Availability

A1.1 Current processing capacity and usage are maintained, monitored, and evaluated to manage capacity demand and to enable the implementation of additional capacity to help meet the entity's availability commitments and system requirements.	
Controls specified by ViaWest, Inc.	**Tests performed**
4.6: On a monthly basis, management meets to review network, power, and physical space capacity for the data centers.	Observed a monthly Capacity Planning meeting and determined that each data center/region was discussed and evaluated based on remaining capacity of physical space and critical infrastructure, including cooling, backup power, and utilities, using current capacity as well as sales projections. Inspected a sample of monthly capacity reports from the various building management, network, and data center systems and meeting agendas to determine whether monthly management meetings were held and reports were distributed and discussed.
Results of Test: No deviations noted.	

Additional Criteria for Availability

A1.2 Environmental protections, software, data backup processes, and recovery infrastructure are authorized, designed, developed, implemented, operated, approved, maintained, and monitored to meet availability commitments and system requirements.	
Controls specified by ViaWest, Inc.	**Tests performed**
5.1: Each data center has implemented the following: HVAC cooling, power distribution units or remote power panels, uninterruptable power supply (UPS) systems, generator(s), and raised floors.	For the data centers physically visited during the examination period, observed the existence of the HVAC systems, power distribution units or remote power panels, UPS systems, generator(s), and raised floors.
5.2: Environmental controls are monitored, and data center staff is alerted of any potential issues.	For the data centers physically visited during the examination period, observed DCCS staff monitoring the data center environmental systems. For the data centers physically visited during the examination period, observed that monitoring systems were enabled on each of the critical support systems. For the data centers physically visited during the examination period, observed that monitoring systems notify the network staff in the event of an incident.
5.3: ViaWest staff tests the generator at least monthly at each data center, and the results are logged and any issues are resolved.	Inquired of the Senior Data Center Manager to determine whether generator tests were performed monthly and whether issues were recorded and resolved. For a sample of monthly generator tests for each in-scope data center, inspected the ViaWest Maintenance database to determine whether data center personnel performed the review and whether any issues identified were resolved.
5.4: ViaWest performs semiannual tests and maintenance for the UPS systems. Any issues identified during the semiannual visit are resolved.	Inquired of the Senior Data Center Manager to determine whether UPS tests and maintenance were performed semiannually and whether issues were recorded and resolved. For a sample of semiannual UPS systems reviews for each data center, inspected the ViaWest Maintenance database to determine whether tests and maintenance were performed and whether data center personnel resolved any issues that were identified.
5.5: ViaWest performs annual checks and maintenance procedures to confirm that fire detection and suppression equipment is working properly at each data center.	Inquired of the Senior Data Center Manager to determine whether fire detection and suppression system tests and maintenance were performed annually and whether issues were recorded and resolved. For a sample of annual fire detection and suppression equipment reviews for each data center, inspected the ViaWest Maintenance database to determine whether tests and maintenance were performed and whether data center personnel resolved identified issues.

Additional Criteria for Availability

A1.2 Environmental protections, software, data backup processes, and recovery infrastructure are authorized, designed, developed, implemented, operated, approved, maintained, and monitored to meet availability commitments and system requirements. (continued)	
Controls specified by ViaWest, Inc.	**Tests performed**
5.6: ViaWest performs tests and maintenance for the HVAC equipment at least quarterly. Any issues identified during the visits are resolved.	Inquired of the Senior Data Center Manager to determine whether HVAC tests and maintenance were performed quarterly and whether issues were recorded and resolved. For a sample of quarterly HVAC tests for each data center, inspected the ViaWest Maintenance database to determine whether maintenance was performed on the equipment and whether data center personnel resolved identified issues.
5.7: ViaWest performs annual tests and maintenance for the power distribution unit (PDU) systems. Any issues identified during the annual visits are resolved.	Inquired of the Senior Data Center Manager to determine whether PDU tests and maintenance were performed annually and whether issues were recorded and resolved. For a sample of annual PDU equipment reviews for each in-scope data center, inspected the ViaWest Maintenance database to determine whether tests and maintenance were performed and whether data center personnel resolved identified issues.
Results of Test: Per inspection of the maintenance logs for the Hillsborough, Portland and Brookwood data centers, the annual PDU preventive maintenance did not occur during the period October 1, 2016 to September 30, 2017. ***Management Response:*** The annual testing was originally scheduled to be performed in September 2017; however, due to vendor availability, it was rescheduled to be performed in October 2017.	

Additional Criteria for Availability

A1.3 Recovery plan procedures supporting system recovery are tested to help meet the entity's availability commitments and system requirements.	
Controls specified by ViaWest, Inc.	**Tests performed**
5.8: Critical network device configurations are backed up using RANCID and Net Line Dancer on a nightly basis.	Obtained a population of network devices from Rancid and Net Line Dancer and the queries used to generate the population and, for a sample of network devices, inspected the log files on RANCID or Net Line Dancer to determine whether: • Net Line Dancer took a snapshot of configuration changes on the device from the previous day • The query used to generate the network device listing contained the appropriate selection criteria
5.9: Managed Services and Client Center Cloud servers are backed up daily. Alerts are configured to notify ViaWest personnel in the event of a backup failure.	Inquired of Backup Engineer to determine whether backups are performed on a regular basis by a backup tool. For a sample day, inspected the backup log for a sample Managed Services client server and a sample Client Center Cloud client server to determine that the backup was completed and replicated to an off-site server. For a sample Managed Services and a sample Client Center Cloud client server, inspected the backup tool to confirm alerts related to failed backups are configured to be sent to client personnel. For a sample failed backup, inspected the Cadence ticket or Nagios alert to determine whether the backup tool automatically generated a ticket and whether the ticket was resolved in a timely manner.
Results of Test: No deviations noted.	