US Signal Company, LLC

System and Organization Controls (SOC) 1 Type 2

Report on Management of US Signal Company, LLC's Description of Its Information Technology General Controls for Its Network and Data Center Services System and on the Suitability of the Design and Operating Effectiveness of Controls

Throughout the Period
July 1, 2023 to June 30, 2024

Contents

I. Independent Service Auditor's Report on a SOC 1 Examination

Tel: 314-889-1100
Fax: 314-889-1101
www.bdo.com

101 South Hanley Road
Suite 800
St. Louis, MO 63105

Independent Service Auditor's Report on a SOC 1 Examination

To the Management of
US Signal Company, LLC
Grand Rapids, Michigan

Scope

We have examined US Signal Company, LLC's (US Signal or service organization) accompanying description of its Information Technology General Controls for Its Network and Data Center Services System (the System) titled *Management of US Signal Company, LLC's Description of Its Information Technology General Controls for Its Network and Data Center Services System* for processing user entities' transactions throughout the period July 1, 2023 to June 30, 2024 (description) and the suitability of the design and operating effectiveness of controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in *Management of US Signal Company, LLC's Assertion* (assertion). The controls and control objectives included in the description are those that management of US Signal believes are likely to be relevant to user entities' internal control over financial reporting. The description does not include aspects of the System that are not likely to be relevant to user entities' internal control over financial reporting.

US Signal uses several Point of Presence facility landlords, subservice organizations, to provide secure facilities for connectivity points. The description includes only the control objectives and related controls of US Signal and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified by US Signal can be achieved only if complementary subservice organization controls assumed in the design of US Signal's controls are suitably designed and operating effectively, along with the related controls at US Signal. Our examination did not extend to controls of the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of US Signal'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.

Service Organization's Responsibilities

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

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description, based on our examination.

Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period July 1, 2023 to June 30, 2024. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- Performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description, based on the criteria in management's assertion.
- Assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description.
- Testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved.
- Evaluating the overall presentation of the description, suitability of the control objectives stated therein, and suitability of the criteria specified by the service organization in its assertion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the System that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in processing or reporting transactions. 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 controls to achieve the related control objectives, is subject to the risk that controls at a service organization may become ineffective.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are listed in Section IV.

Opinion

In our opinion, in all material respects, based on the criteria described in US Signal Company, LLC's assertion:

a. The description fairly presents US Signal's Information Technology General Controls for Its Network and Data Center Services System that was designed and implemented throughout the period July 1, 2023 to June 30, 2024.

b. The controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period July 1, 2023 to June 30, 2024 and if the subservice organizations and user entities applied the complementary controls assumed in the design of US Signal's controls throughout the period July 1, 2023 to June 30, 2024.

c. The controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period July 1, 2023 to June 30, 2024 if complementary subservice organization controls and complementary user entity controls assumed in the design of US Signal's controls operated effectively throughout the period July 1, 2023 to June 30, 2024.

Restricted Use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of US Signal, user entities of US Signal's system during some or all of the period July 1, 2023 to June 30, 2024, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatement of user entities' financial statements.

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

BDO USA, P.C.

September 10, 2024

II. Management of US Signal Company, LLC's Assertion

Management of US Signal Company, LLC's Assertion

We have prepared the accompanying description of US Signal Company, LLC's (US Signal or service organization) Information Technology General Controls for Its Network and Data Center Services System (the System) titled *Management of US Signal Company, LLC's Description of Its Information Technology General Controls for Its Network and Data Center Services System* for processing user entities' transactions throughout the period July 1, 2023 to June 30, 2024 (description) for user entities of the System during some or all of the period July 1, 2023 to June 30, 2024 and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by the subservice organizations and user entities of the System themselves, when assessing the risks of material misstatement of user entities' financial statements.

US Signal uses several Point of Presence facility landlords, subservice organizations, to provide secure facilities for connectivity points. The description includes only the control objectives and related controls of US Signal and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified by US Signal can be achieved only if complementary subservice organization controls assumed in the design of US Signal's controls are suitably designed and operating effectively, along with the related controls at US Signal. The description does not extend to controls of the subservice organizations.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of US Signal's controls are suitably designed and operating effectively, along with related controls at the service organization. The description does not extend to controls of the user entities.

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

a. The description fairly presents the Information Technology General Controls for Its Network and Data Center Services System made available to user entities of the System during some or all of the period July 1, 2023 to June 30, 2024 for processing their transactions as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description:

    i. Presents how the System made available to user entities of the System was designed and implemented to process relevant user entity transactions, including, if applicable:

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

        (2) The procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports, and other information prepared for user entities of the System.

        (3) The information used in the performance of the procedures, including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities.

(4) How the System captures and addresses significant events and conditions other than transactions.

(5) The process used to prepare reports and other information for user entities.

(6) Services performed by a subservice organization, if any, including whether the inclusive method or the carve-out method has been used in relation to them.

(7) The specified control objectives and controls designed to achieve those objectives, including, as applicable, complementary subservice organization controls and complementary user entity controls assumed in the design of the service organization's controls.

(8) Other aspects of our control environment, risk assessment process, information and communications (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.

ii. Includes relevant details of changes to the service organization's system during the period covered by the description.

iii. 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 user entities of the System and their user auditors and may not, therefore, include every aspect of the System that each individual user entity of the System and its auditor may consider important in its own particular environment.

b. The controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period July 1, 2023 to June 30, 2024 to achieve those control objectives if the subservice organizations and user entities applied the complementary controls assumed in the design of US Signal's controls throughout the period July 1, 2023 to June 30, 2024. The criteria we used in making this assertion were that:

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

ii. The controls identified in the description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved.

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

US Signal Company, LLC

September 10, 2024

III. Management of US Signal Company, LLC's Description of Its Information Technology General Controls for Its Network and Data Center Services System

Management of US Signal Company, LLC's Description of Its Information Technology General Controls for Its Network and Data Center Services System

Overview

This is a System and Organization Controls (SOC) 1 Type 2 report on US Signal Company, LLC's (US Signal, service organization, or Company) Information Technology (IT) General Controls for Its Network and Data Center Services System (the System) for processing user entities' transactions throughout the period July 1, 2023 to June 30, 2024, which may be relevant to the internal control over financial reporting of user entities. The description has been prepared in accordance with the guidance issued by the AICPA, specifically, AT-C Section 320, Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting.

Company and Services Overview

US Signal is a digital infrastructure company offering network connectivity, cloud hosting, colocation, data protection, security, and disaster recovery solutions, all powered by its wholly owned and operated robust, fiber network. US Signal also helps customers optimize their IT resources through managed and professional services.

Services Provided

The Company's product and service offerings include cloud hosting, colocation, data protection, security, and disaster recovery solutions, in addition to its network services.

Scope

This description addresses only US Signal's IT General Controls for Its Network and Data Center Services System provided to user entities and excludes other services provided by US Signal. The description is intended to provide information for user entities of the System and their independent auditors who audit and report on such user entities' financial statements, to be used in obtaining an understanding of the System and the controls over that system that are likely to be relevant to user entities' internal control over financial reporting. The description of the System includes the IT general controls that support the delivery of US Signal's system. The description does not encompass all aspects of the services provided or procedures followed that are unrelated to internal control over financial reporting activities performed at US Signal.

In addition to US Signal's headquarters in Grand Rapids, Michigan, the system's scope includes the following US Signal data center facilities:

Michigan	Indiana	Illinois	Wisconsin
Detroit Metro	Indianapolis	Oak Brook	Madison
Grand Rapids East	South Bend		
Grand Rapids South			
Southfield			

US Signal uses several Point of Presence (POP) facility landlords, subservice organizations, to provide secure facilities for connectivity points. The description includes only the control objectives and related controls of US Signal and excludes the control objectives and controls of the subservice organizations.

US Signal was acquired by Igneo Infrastructure Partners in February 2023. US Signal remains an independent entity and is responsible for the services to its clients as well as the controls related to the Network and Data Center Services System as it pertains to the scope of this report. Controls performed by Igneo Infrastructure Partners are not included in the scope of this report.

Internal Control Framework

This section provides information about the five interrelated components of internal control at US Signal: control environment, risk assessment process, monitoring activities, information and communications, and control activities.

US Signal's internal control components include controls that may have a pervasive effect on the organization, specific processes, account balances, disclosures, classes of transactions, or applications. Some of the components of internal control have more of an effect at the entity level, while other components are primarily related to specific processes or applications.

Control Environment

Commitment to Integrity and Ethical Values

US Signal has a documented Business Conduct Policy within the Employee Handbook that defines employee conduct standards. The Employee Handbook is posted on the intranet and made available for employees to view. Employees are required to sign an acknowledgement stating they have read, understand, and agree to comply with the responsibilities and requirements outlined within the Employee Handbook and US Signal policies upon hire and annually thereafter.

Individuals offered positions at US Signal are subject to background checks as part of the employee screening process.

US Signal has an anonymous policy-violation complaint form available to internal users on the intranet. Compliance Management is automatically notified and monitors workforce member complaints reported via the form.

Independent Oversight

The roles and responsibilities of the US Signal Board of Directors are segregated from the roles and responsibilities of management. The Board is independent of the day-to-day operations of control owners and serves in an oversight capacity of the line management overseeing those control owners. The Chief Information Security Officer provides oversight of the development and performance of internal control through oversight of the Internal Audit Program and the Information Security Program, which drives the execution of US Signal's Governance, Risk, Compliance, and Security Program. The Chief Information Security Officer reports results directly to the Board of Directors and Executive Leadership of US Signal.

In addition, the US Signal Board of Directors has established an audit subcommittee, which is responsible for oversight of the Internal Audit and Information Security Programs at US Signal. The Board of Directors and subcommittees meet to discuss and monitor progress in the areas of audit, compensation, governance, risk, strategy, and other topics as needed on at least a quarterly basis.

Organizational Structure

US Signal maintains up-to-date reporting lines and levels of authorities within the organization's HR information system, which is made available for employees to view. The roles and responsibilities, as well as the knowledge and skills that are needed to perform them, are defined in written job descriptions. During the hiring process, management reviews job descriptions to ensure that the candidates possess the required qualifications to perform the duties outlined in the job description. The responsibility and accountability for updating and maintaining US Signal information security policies are assigned to the Chief Information Security Officer and Executive Leadership. US Signal policies are reviewed annually and updated as necessary.

Resource Planning

On an at least annual basis, management performs people and resource planning to ensure appropriate staff and resources are available to meet the Company's objectives and presents to the Board of Directors for approval. If it is determined that additional resources are needed, the new hire and/or asset acquisition processes are initiated.

Employee Performance and Training

Employee performance is evaluated on an annual basis to determine that employees are qualified to fulfill their job responsibilities. Employees are also required to complete security awareness training when hired and on an annual basis thereafter. If an individual is deemed to not be meeting the qualifications of the job position, including not completing necessary trainings, US Signal has a documented Progressive Discipline Policy within the Employee Handbook, which is used to outline procedures around how they address conduct issues. When conduct issues occur, a discipline form is completed to document the issue and is communicated to the employee, their supervisor, and HR.

Risk Assessment Process

US Signal recognizes the importance of risk management in properly managing corporate and customer assets and providing high-quality, cost-effective services to its customers. To assist with this, management maintains a list of objectives and contractual commitments that is reviewed and updated on at least an annual basis to ensure that they are documented with sufficient clarity. US Signal monitors service-level statistics on at least a quarterly basis to ensure that they are meeting company objectives. Results of the monitoring are communicated to management for review.

Management subscribes to external reporting services that identify changes to technology or regulations relating to services provided by US Signal. Additionally, the Chief Information Security Officer maintains an Information Technology road map that outlines the organization IT strategic objectives and projects. The road map is reviewed and updated by management on an at least annual basis.

US Signal performs a risk assessment over their environment on an annual basis to identify potential threats that would impair system security and availability and analyze the risk associated with the identified threats and determine mitigation strategies for those risks. US Signal management meets to review the results of operations, audits, and to discuss the risk assessment, including identifying new risks and developing and implementing appropriate measures to address new risk at least on a quarterly basis. In addition to the overall risk assessment, US Signal documents risks for each new or changed line of business to identify potential vulnerabilities and threats specific to each service they provide. The product-specific risk assessments are updated on an as-needed basis.

As part of the annual risk assessment, management assesses fraud risk to identify the various ways that fraud and misconduct can occur within their environment, including how management might engage in inappropriate actions, and maintains documentation of this assessment.

Through its ongoing and annual risk-assessment process, US Signal evaluates changes in the regulatory and physical environment in which US Signal operates, as well as vendor and business-partner relationships.

Monitoring Activities

Management performs ongoing evaluations on a day-to-day basis to monitor the effectiveness of controls and functions of the organization. From these evaluations, US Signal develops an audit schedule annually to assist with identifying and monitoring the various levels of risk within the organization. Based on the audit schedule, US Signal performs various self-certification audits annually to test the design and operating effectiveness of controls within the environment. Audit reports are generated to document their procedures and results of the self-certification audits. US Signal performs an internal assessment of their controls against the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) on at least an annual basis. Results of the assessment are reviewed by management to ensure that components of internal controls are present and functioning.

In addition to the audits above, US Signal audits their data center facilities on an annual basis to ensure that the appropriate controls are in place and operating effectively at the facilities.

The results of internal assessments are communicated to the CEO or executive leadership at least annually.

US Signal has a documented Vendor Management Policy that outlines its vendor due-diligence procedures. Based on the policy, US Signal performs annual due diligence on high-risk vendors to ensure the risk associated with vendors is managed.

Information and Communications

US Signal has implemented policies and procedures relevant to information security, and based on those policies and procedures, performs logical and physical security, change management, incident monitoring, and retention control activities, to ensure that the systems supporting the functioning of internal control are producing relevant, quality information.

Internal Communication

US Signal uses various methods of communication within the Company to ensure that employees understand their individual roles and responsibilities as they relate to the network and data center services. These methods include orientation and training, the use of electronic mail messages to communicate time-sensitive information, systems of record, and the use of diagnostic applications to monitor services and automatically alert staff when issues arise.

Descriptions of US Signal's systems are posted on the Company's intranet and are available to internal users to view. The descriptions delineate the boundaries of the systems and key aspects of processing.

To communicate the incident response procedures to internal users, US Signal has developed an Incident Response Policy that outlines steps that need to be taken when incidents are identified. The policy is posted online and available for internal users to view. US Signal has also implemented formal customer support and incident management policies and procedures that document how customer service issues are handled. The policy is posted in the US Signal file directory and available for internal users to view.

In order to ensure that internal users are aware of changes that are being made within the environment, US Signal conducts a biweekly maintenance meeting and maintains a system-change calendar that identifies and communicates planned changes. The calendar is posted and available for internal users to view through a shared Microsoft (MS) Outlook calendar. System changes that affect US Signal services are communicated to applicable internal and external users as part of the implementation process.

External Communication

System descriptions are available to external users through the customer portal that delineate the boundaries of the system and describe relevant components, as well as its purpose and design. Agreements are established with service providers and business partners that include clearly defined terms, conditions, and responsibilities for service providers and business partners. In addition, products and services offered by US Signal have documented SLAs that are made available to customers on the US Signal website.

US Signal's security, availability, and confidentiality responsibilities and commitments are communicated to external users within master agreements.

Customers are provided information on how to report security events and service-related issues via phone, email, or through creating a trouble ticket through the customer portal to the Technical Operations Center (TOC) on the US Signal website.

Information Systems — Corporate Systems and Network

US Signal employs a local area network (LAN) topography that provides connectivity between servers and workstations. Email, file, and print sharing and general access are provided to domain users. The LAN is connected to the wide area network (WAN) via redundant next-generation firewalls. Access through the firewalls is default deny-all, with allowance for business-approved protocols and traffic such as normal web traffic (Hypertext Transfer Protocol Secure [HTTPS], file transfer protocol [FTP], simple mail transfer protocol [SMTP], etc.,) and is monitored via an intrusion

prevention system (IPS) and an intrusion detection system (IDS). The Company uses virtual private network (VPN) connectivity with Secure Sockets Layer (SSL) encryption technology and two-factor authentication to secure the network and enhance security. Primary corporate servers are Windows Server 2019 and above. Servers include, but are not limited to, primary and secondary domain controllers, Great Plains, and File Share. The primary operating system on workstations is Microsoft Windows.

Information Systems — Network

US Signal provides a secure environment for network services and follows a strict physical and virtual access control policy that limits which personnel can access production servers and data. Only authorized US Signal employees can access a client's information maintained on the servers. IT or Engineering Operations staff monitors access to all servers, routers, switches, and any other devices that interact with customer data. The servers are monitored 24/7/365 and are physically accessible only via proximity card or biometric access system authentication.

Information Systems — Infrastructure Components

US Signal uses multiple methods to keep management and customer traffic separate and provide a secure and redundant network architecture. These methods include virtual routing and forwarding (VRF) and virtual LANs (VLAN), or even separate physical networks where appropriate. Network Engineers monitor network components for security, capacity, and performance issues. Additional control procedures include:

- Full infrastructure redundancy for routers, switches, firewalls, and other network components.
- Secure, hardened operating systems.
- Real-time monitoring and reporting tools.
- Capacity planning and utilization monitoring.

Control Objectives and Related Control Activities

The service organization has developed a variety of policies and procedures, including related control activities, to help ensure that the service organization's objectives are carried out and that risks are mitigated. These control activities help ensure that services are administered in accordance with the service organization's policies and procedures.

Control activities are performed at multiple levels throughout the organization and at various stages during the relevant business process. Controls may be preventive or detective in nature and may encompass a range of manual and automated controls, including authorizations, reconciliation, and IT controls. Duties and responsibilities are allocated among personnel to ensure that a proper segregation of duties is maintained.

US Signal has specified the control objectives and identified the controls that are designed to achieve the related control objectives below. Numerical cross-references are used to reference controls in Section III to the related control and testing in Section IV.

Control Objective 1 — Customer Setup and Implementation

Controls provide reasonable assurance that new client infrastructure being set up and subsequent changes to the existing client infrastructure are authorized and completely and accurately implemented.

US Signal maintains process and procedure documents that provide structure and guidelines for the customer order process. The guidelines described in the process and procedure documents apply to new service and changes to existing client infrastructure, including moving, adding additional service, or modifying an existing service, as well as disconnecting customer circuits and destroying managed data centers that are no longer needed. Policy and procedures are posted on the company intranet for employees to reference when needed (1.1).

When new clients engage US Signal as their service provider or an existing client requests a change to their service, the sales representative completes an Order for Service (OFS), which is submitted to Service Delivery via the Web OFS portal. A manager within the Service Delivery Department will authorize a sale within the Web OFS system and enter information into the Order Management system when the necessary documents have been received. The OMNI application Order Management module will not accept the order until key fields are entered (1.2).

Orders are then assigned to a project manager, who will be responsible for the completion of tasks required to complete the order. Depending on the type of service requested, the project manager coordinates with the necessary department team leaders, such as the Circuit Design and Provisioning team, engineering, field operations, and external partners, such as local exchange companies, to complete the order. Requests to implement new or change existing customer equipment are documented within project checklists, where a project manager verifies the appropriate steps are completed based on the type of request, including testing and authorization by the customer (1.3). Appropriate steps include verifying circuit orders are provisioned and tested, customer premise equipment (CPE) is installed and tested, and the provisioning team implements the required managed data center elements, including virtual servers, storage, and networks.

Once the order has been implemented, the project manager will send an Order Completion Notice to the customer via email acknowledging that their order has been completed and is available to be used (1.4).

Control Objective 2 — Customer Support and Incident Management

Controls provide reasonable assurance that customer service issues are identified, tracked, recorded, and resolved in a complete and accurate manner.

US Signal has implemented formal customer support and incident management policies and procedures that document how customer service issues are handled. The policy is posted in the US Signal file directory and available for internal users to view (2.1).

Customers are provided information on how to report security events and service-related issues via phone, email, or through creating a trouble ticket through the customer portal to the Technical Operations Center (TOC) on the US Signal website (2.2). The TOC is staffed 24 hours a day, seven days a week, in order to support customers as service-related issues occur (2.3).

Requests for customer support are recorded and processed through US Signal's internal ticket system. Once a service issue or security event is identified and reported to the TOC, a ticket is generated in the ticket system and the TOC personnel will document the following relevant details:

- Contact information (reporting party information, premise contact/access information, etc.)
- Impact on the customer
- Type (complete loss of service, impairment, technical support, internal, etc.)
- Incident subtype (repair, monitor, network outage, technical support, etc.)
- Incident group designation (the responsible group within US Signal)
- Incident status (open, vendor-referred, customer-referred, monitor, cleared, closed-resolved)

In addition, incident details and notes are documented in the incident ticket whenever an update is received and/or communication is made regarding the underlying ticket. These notes are automatically timestamped to provide an accurate tracking and progression analysis. TOC personnel document service issues that have been identified and reported to them through the Network Management System (NMS) or by internal and external users within a ticketing system. TOC personnel review the issue and close a ticket once the item has been addressed (2.4).

Escalations are made internally if management involvement is deemed necessary in order to expedite an event remedy to address service issues. TOC management is automatically notified of any issues or events that have been escalated by the TOC personnel (2.5).

TOC maintenance management analyzes ticketing and customer call data on a monthly basis to assess the quality of customer service and to identify trends, including whether tickets are acknowledged and resolved in a timely manner (2.6).

Control Objective 3 — Managed Customer Premise Equipment

Controls provide reasonable assurance that managed customer premise equipment relevant to user entities' internal control over financial reporting is configured to be monitored according to contract specifications.

US Signal maintains formalized policies and procedures that direct personnel on how to respond to incidents related to managed equipment (3.1).

US Signal's equipment that monitors managed CPE is configured to log and trap link status to the NMS. If a managed CPE does not communicate to the monitoring equipment, the link status of the CPE is logged in the NMS, and the TOC receives the underlying Managed Service Alarm(s) and responds in accordance with established policies and procedures to ensure that the stated contract specifications for the service is provided (3.2).

Control Objective 4 — Data Storage and Destruction

Controls provide reasonable assurance that procedures are in place and followed for the secure storage and destruction of sensitive data to protect data relevant to user entities' internal control over financial reporting.

Policies and Procedures

US Signal has a formalized Data Protection Policy document that defines how data will be securely stored and destroyed. The policy is reviewed and updated annually (4.1).

Data Storage

Customer data storage is segregated into individual virtual storage repositories so that customers do not have access to other customers' data (4.2).

Data Destruction

Customers execute a master services agreement with US Signal which defines the data retention and destruction rules for customer data. Upon termination of services, US Signal will return or delete customer data in accordance with the agreement (4.3). US Signal performs a quarterly data audit to ensure data destruction procedures are being followed (4.4).

Control Objective 5 — Logical Access to Production Network and Managed Data Center Elements

Controls provide reasonable assurance that logical access to the US Signal production network and managed data center elements relevant to user entities' internal control over financial reporting is restricted to authorized and appropriate individuals.

User Modifications

HR personnel or Department Managers submit requests for access to the production network elements to the IT Helpdesk who validate the request was properly authorized and configure access in the production (RADIUS) server (5.1). Upon employee termination, the IT Helpdesk removes access to US Signal systems after being notified of the termination by HR personnel (5.2).

Production Network Element Security

Remote access to the US Signal internal network is permitted for Active Directory users via VPN connectivity with Duo Security two-factor authentication connectivity (5.3). Access to production network elements is configured to be restricted to specific protocols, ports, and IP addresses (5.4).

Access to the individual production network elements and managed CPE is authenticated through a centralized RADIUS server (5.5). Access to the RADIUS server, which restricts access to the production network elements, is configured to authenticate via Active Directory (5.6). Network password restrictions are enabled for password length, strength, duration, history, and lockout settings (5.7).

Logging and monitoring of security events and system alerts are enabled on network elements and are configured to log activity to an internal Security Information and Event Management (SIEM) and the Company's NMS (5.8). Security alerts from the NMS are monitored in real time by the TOC (5.9).

Managed Data Center Element Security

Access to manage the virtual components for the managed data center services is restricted through the Management Console, which is configured to authenticate users using lightweight directory access protocol (LDAP) (5.10). Users with the ability to access the vSphere are limited to authorized and appropriate IT personnel based on job responsibilities (5.11).

Privileged access to the network, applications, application databases, secured network drives, and back-end supporting systems is reviewed by management on a quarterly basis to ensure that privileged access is restricted to appropriate users based on their job responsibilities. Any access modifications needed as a result of the review are made by management (5.12).

Additionally, user access to the network is reviewed on a quarterly basis by management to ensure that access is restricted to appropriate users based on job responsibilities. Any access modifications needed as a result of the review are made by management (5.13).

Control Objective 6 — Physical Security and Environmental Controls

Controls provide reasonable assurance that physical access to the US Signal data center facility containing the production servers and telecommunication equipment used to deliver the managed data center service is restricted to properly authorized individuals and environmental controls exist to protect these resources.

Physical Security

Access to the corporate headquarters and data center facilities containing production servers and telecommunications equipment is controlled and restricted by an electronic proximity card or biometric access system (6.1). In addition to the electronic proximity card or biometric access system, the data center facilities' camera and alarm systems are monitored on an ongoing basis by the TOC. Camera and alarm systems are in place at each data center facility to ensure each location is secured and monitored (6.2).

Granting access to the data center facilities follows two processes, depending on who is requesting the access. For employees, requests for new access or changes to existing access are submitted to the Facilities Department from HR personnel. For customers and vendors, requests for new access or changes to existing access are submitted to the Facilities Department from the customer's or vendor's designated point of contact. Facilities personnel validate the request and create the new user's access based on the request (6.3). When employees leave the organization, HR personnel reclaim the terminated employee's access card and notify the Facilities Department via email or ticket so that physical access privileges, such as biometrics or proximity card, will be revoked (6.4). Customers are responsible for notifying US Signal when physical access should be terminated for their employees. When US Signal receives a request for removal of customer access to the data center, a ticket is created to track the removal of physical access (6.5).

Physical access to the corporate headquarters and data center facilities is reviewed on a quarterly basis by management. Any access modifications needed as a result of the review are made by management (6.6).

Environmental Controls

Fire and smoke detectors, automated clean-agent or pre-action wet fire suppression systems, and hand-held fire extinguishers are in place to protect US Signal data center facilities from fire-related hazards (6.7). The data center facilities feature dedicated climate control systems to control the temperature and humidity within the facilities (6.8). Additionally, uninterruptible power supply (UPS) units and power generation equipment protect the server and telecommunication equipment from power surges and sudden power outages (6.9).

Control Objective 7 — Logical Security - Internal Systems

Controls provide reasonable assurance that logical access to the US Signal internal systems relevant to user entities' internal control over financial reporting is restricted to authorized individuals and is implemented and maintained according to internal specifications and such individuals are restricted to performing authorized and appropriate actions.

User Modifications

HR personnel or Department Managers submit requests for new-user access to the domain to the IT Helpdesk through an email or ticket. The IT Helpdesk Analyst validates the request and creates the new user's accounts with the appropriate access based on the user's role and access requested (7.1). Additionally, when a user needs access to internal systems, HR personnel or Department Managers submit requests for new user access to the OMNI application to the IT Helpdesk through an email or ticket. The IT Helpdesk Analyst validates the request and creates or modifies the user's account with the appropriate access based on the user's role and access requested (7.2). Upon employee termination, the IT Helpdesk removes access to US Signal systems after being notified of the termination by HR personnel (7.3).

Active Directory Security

In accordance with the US Signal Information Security Policy, users with access to US Signal systems require a uniquely assigned identifiable user ID (7.4). User IDs are based on a combination of user characteristics and are specific to a user. Network password restrictions are enabled for password length, strength, duration, history, and lockout settings (7.5). The ability to create or modify users and user access privileges is limited to authorized and appropriate IT personnel based on job responsibilities (7.6).

Potential Active Directory security violations, including users gaining administrative access to the system, are logged within the SIEM (7.7).

OMNI Application Security

OMNI utilizes unique user IDs and passwords to authenticate and authorize users. OMNI password parameters are in place and are set to require minimum length, complexity, expiration, history, and lockout settings (7.8).

Privileged access to the network, applications, application databases, secured network drives, and back-end supporting systems is reviewed by management on a quarterly basis to ensure that privileged access is restricted to appropriate users based on their job responsibilities. Any access modifications needed as a result of the review are made by management (7.9). User access to the network is reviewed on a quarterly basis by management to ensure that access is restricted to appropriate users based on job responsibilities. Any access modifications needed as a result of the review are made by management (7.10).

Control Objective 8 — Corporate Network Security

Controls provide reasonable assurance that corporate connections to the internet or other networks relevant to user entities' internal control over financial reporting are protected from unauthorized access.

Internal US Signal Network

US Signal has firewalls at the perimeter of their network to protect their corporate systems from external threats. These firewalls have been configured to protect the perimeter connection, interconnections with customers' networks, and secure network entry points within the organization (8.1). The firewalls have been configured to analyze the data and packets that are routed through the network and deny access to unauthorized traffic (8.2).

Intrusion Detection Systems

The firewalls include intrusion prevention features to detect and alert on potential threats. Specific thresholds are defined within the IDS/IPS tools, and a breach of those thresholds automatically sends logs to a log aggregation tool and alerts US Signal of potential threats (8.3).

Network Monitoring

US Signal utilizes a firewall equipped with an analysis tool to monitor network security, bandwidth, and performance issues. The analysis tool examines firewall logs and generates real-time reports to assist the Network Engineers in performing forensic analysis, capacity planning, and policy enforcement. If a network component goes offline, an automated alert is sent to the TOC through the NMS application (8.4).

Wireless

US Signal uses Wi-Fi Protected Access 2 (WPA2) encryption on wireless network connections, and access is limited to Active Directory users (8.5).

Remote Access

Remote access to the US Signal internal network is permitted for Active Directory users via VPN connectivity with Duo security two-factor authentication connectivity (8.6).

Endpoint Protection

Endpoint protection software protects production and email servers, workstations, and network-connected laptops against viruses and other malicious code (8.7). The endpoint protection software is configured to monitor data and traffic on production and email servers, workstations, and

network-connected laptops with virus signature definitions that are automatically updated from the vendor (8.8). US Signal has a predefined listing of software that is prohibited from being installed on Company laptops and workstations. Software on the predefined listing is automatically uninstalled, and IT is alerted (8.9).

Complementary Subservice Organization Controls

In some instances, a service organization's controls cannot provide reasonable assurance that its control objectives were achieved without the subservice organizations performing certain activities in a defined manner. Such activities are referred to as complementary subservice organization controls (CSOCs). The following CSOCs are those controls that US Signal's management assumed, in the design of the System, would be implemented by a subservice organization and are necessary, in combination with controls at US Signal, to provide reasonable assurance that the service organization's control objectives are achieved.

Number	CSOC	Applicable Control Objective
Point of Presence Facility Landlords		
1.	Physical access to the POP facilities is restricted to authorized personnel.	CO8
2.	Appropriate environmental controls such as air conditioning, alternate power supply, fire extinguishers, and fire alarms are implemented, monitored, and maintained.	CO8

Complementary User Entity Controls

In some instances, a service organization's controls cannot provide reasonable assurance that its control objectives were achieved without user entities performing certain activities in a defined manner. Such activities are referred to as complementary user entity controls (CUECs). The following CUECs are those controls that US Signal's management assumed, in the design of the System, would be implemented by user entities and are necessary, in combination with controls at US Signal, to provide reasonable assurance that the service organization's control objectives are achieved.

Number	CUEC	Applicable Control Objective
1.	User entities are responsible for notifying US Signal of changes to contact information in a timely manner.	CO1
2.	User entities are responsible for ensuring that identified problems are tracked and reported to the US Signal TOC, as required by the SLA, and for tracking those problems.	CO2
3.	User entities are responsible for ensuring only appropriate users have the ability to submit data destruction requests to US Signal.	CO4

Number	CUEC	Applicable Control Objective
4.	User entities are responsible for ensuring that appropriate logical security controls are in place on their virtual servers at the operating system, application, database, and network levels.	CO5
5.	User entities are responsible for notifying US Signal Facilities Department of access changes to the data center facilities in a timely manner. User entities are also responsible for reviewing and approving access listings generated by US Signal Facilities Department on an annual basis.	CO6

IV. US Signal Company, LLC's Description of Its Control Objectives and Related Controls, and Independent Service Auditor's Tests of Controls and Results of Tests

US Signal Company, LLC's Description of Its Control Objectives and Related Controls, and Independent Service Auditor's Tests of Controls and Results of Tests

This report, when combined with an understanding of the controls at user entities, is intended to assist auditors in planning the audit of user entities' financial statements or user entities' internal control over financial reporting and in assessing control risk for assertions in user entities' financial statements that may be affected by controls at US Signal. The examination was performed in accordance with attestation standards established by the AICPA, specifically, AT C Section 320, Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting.

Our examination was limited to the control objectives and related controls specified by US Signal in Section IV of this report and did not encompass all aspects of the services provided or controls of US Signal or extend to controls performed by user entities. Unique processes or control situations not included in the description are outside the scope of this examination.

It is the responsibility of each user entity and its independent auditor to evaluate this information in conjunction with the evaluation of internal control over financial reporting at the user entity in order to assess the total internal control. If internal control is not effective at user entities, US Signal's controls may not compensate for such weaknesses.

The scope of the examination included tests of the operating effectiveness of controls over US Signal's IT General Controls for Its Network and Data Center Services System, including controls related to changes to the System applications, but did not include tests related to the functioning of or calculations performed by the software used in the delivery of the System or of reports generated by the software.

US Signal's internal control represents the collective effect of various factors on establishing or enhancing the effectiveness of the controls specified by US Signal. In planning the nature, timing, and extent of our testing of the controls to achieve the control objectives specified by US Signal, we considered aspects of US Signal's control environment, risk assessment process, monitoring activities, and information and communications.

Tests of Controls

Our testing of controls was restricted to the controls specified by US Signal and was not extended to controls performed by user entities or other controls that were not documented as tested under each control objective listed in this section of the report.

The description of tests of controls and results of those tests are presented in this section of the report and are the responsibility of BDO USA, P.C., the service auditor. The description of the control objectives, the related controls, and the complementary subservice organization and user entity controls to achieve the objectives have been specified by, and are the responsibility of US Signal.

The basis for all tests of operating effectiveness includes inquiry of the individual(s) responsible for the control. As part of our testing of each control, we inquired of the individual(s) to determine the fairness of the description of the control and to evaluate the design and implementation of the

control. As part of our inquiries, we also gained an understanding of the knowledge and experience of the personnel managing the control(s) and corroborated evidence obtained as part of other testing procedures. While inquiries were performed for every control, our inquiries were not listed individually for every control activity tested and shown in Section IV.

Additional testing of the control activities may have been performed using the following methods:

Method	Description
Inquiry	Inquired of appropriate personnel and corroborated responses with management.
Observation	Observed the application, performance, or existence of the specific control(s), as represented by management.
Inspection	Inspected documents and records indicating performance of the control.
Reperformance	Reperformed the control or processing application to ensure the accuracy of its operation.

When using information produced by the service organization, we evaluated whether the information was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes.

Control Objective 1 – Customer Setup and Implementation

Controls provide reasonable assurance that new client infrastructure being set up and subsequent changes to the existing client infrastructure are authorized and completely and accurately implemented.

Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
1.1	US Signal maintains process and procedure documents that provide structure and guidelines for the customer order process. The guidelines described in the process and procedure documents apply to new service and changes to existing client infrastructure, including moving, adding additional service, or modifying an existing service, as well as disconnecting customer circuits and destroying managed data centers that are no longer needed. Policy and procedures are posted on the company intranet for employees to reference when needed.	Inspected the Service Delivery Implementation Process document to determine that a formalized process was in place that documented new customer setup and implementation, changes to existing client infrastructure, and modifying an existing service.	No exceptions noted.
		Inspected the Data Destruction Procedure document to determine that a formalized procedure was in place that documented disconnecting customer circuits and destroying managed data centers that were no longer needed.	No exceptions noted.
		Inspected the US Signal company intranet to determine that process and procedure documents were posted and available for employees to reference when needed.	No exceptions noted.
1.2	A manager within the Service Delivery Department will authorize a sale within the Web OFS system and enter information into the Order Management system when the necessary documents have been received. The OMNI application Order Management module will not accept the order until key fields are entered.	Inspected the OFS authorization log for a selection of orders for new equipment or changes to existing services to determine that a manager within the Service Delivery Department authorized the sale.	No exceptions noted.
		Observed a test sale being entered into the Order Management system to determine that key fields related to the customer order were required by the system before an order could be accepted.	No exceptions noted.

Control Objective 1 – Customer Setup and Implementation

Controls provide reasonable assurance that new client infrastructure being set up and subsequent changes to the existing client infrastructure are authorized and completely and accurately implemented.

Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
1.3	Requests to implement new or change existing customer equipment are documented within project checklists, where a project manager verifies the appropriate steps are completed based on the type of request, including testing and authorization by the customer.	Inspected the project manager checklist and supporting documentation for a selection of orders for new equipment or changes to existing services to determine that a project manager completed the checklist and documented the completion of the appropriate steps for the order.	No exceptions noted.
1.4	Once the order has been implemented, the project manager will send an Order Completion Notice to the customer via email acknowledging that their order has been completed and is available to be used.	Inspected the Order Completion Notice for a selection of orders for new equipment or changes to existing services to determine that a notification was sent to the customer upon completion of the order.	No exceptions noted.

Control Objective 2 – Customer Support and Incident Management

Controls provide reasonable assurance that customer service issues are identified, tracked, recorded, and resolved in a complete and accurate manner.

Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
2.1	US Signal has implemented formal customer support and incident management policies and procedures that document how customer service issues are handled. The policy is posted in the US Signal file directory and available for internal users to view.	Inspected the TOC maintenance overview document to determine that procedures had been established to address customer support issues.	No exceptions noted.
		Inspected the file directory to determine the TOC maintenance overview document was available for internal users to view.	No exceptions noted.
2.2	Customers are provided information on how to report security events and service-related issues via phone, email, or through creating a trouble ticket through the customer portal to the TOC on the US Signal website.	Inspected the US Signal website to determine a published phone number and email address were available for customers to report security events and service-related issues.	No exceptions noted.
		Inspected the customer portal to determine customers were able to create a trouble ticket to report security events and service-related issues.	No exceptions noted.
2.3	The TOC is staffed 24 hours a day, seven days a week, in order to support customers as service-related issues occur.	Inspected the TOC personnel schedule to determine that TOC personnel were scheduled 24 hours a day, seven days a week.	No exceptions noted.
2.4	TOC personnel document service issues that have been identified and reported to them through the NMS or by internal and external users within a ticketing system. TOC personnel review the issue and close a ticket once the item has been addressed.	Inspected the TOC ticket for a selection of service issues identified and reported to the TOC to determine TOC personnel reviewed the issue and closed the ticket once the item had been addressed.	No exceptions noted.

Control Objective 2 – Customer Support and Incident Management

Controls provide reasonable assurance that customer service issues are identified, tracked, recorded, and resolved in a complete and accurate manner.

Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
2.5	Escalations are made internally if management involvement is deemed necessary in order to expedite an event remedy to address service issues. TOC management is automatically notified of any issues or events that have been escalated by the TOC personnel.	Inspected evidence of a TOC ticket getting escalated within the ticketing system to determine that TOC management was automatically notified.	No exceptions noted.
2.6	TOC maintenance management analyzes ticketing and customer call data on at least a monthly basis to assess the quality of customer service and to identify trends, including whether tickets are acknowledged and resolved in a timely manner.	Inspected the TOC Maintenance Statistics report for a selection of months to determine that TOC management analyzed ticketing and customer data at least monthly.	No exceptions noted.

Control Objective 3 – Managed Customer Premise Equipment

Controls provide reasonable assurance that managed customer premise equipment relevant to user entities' internal control over financial reporting is configured to be monitored according to contract specifications.

Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
3.1	US Signal maintains formalized policies and procedures that direct personnel on how to respond to incidents related to managed equipment.	Inspected the TOC maintenance overview document to determine that policies and procedures existed to instruct personnel on how to respond to incidents related to managed equipment.	No exceptions noted.
3.2	US Signal's equipment that monitors managed CPE is configured to log and trap link status to the NMS. If a managed CPE does not communicate to the monitoring equipment, the link status of the CPE is logged in the NMS, and the TOC receives the underlying Managed Service Alarm(s) and responds in accordance with established policies and procedures to ensure that the stated contract specifications for the service is provided.	Inspected the NMS dashboards to determine that CPE log and trap link status was configured to be monitored within the NMS.	No exceptions noted.
		Inspected the NMS alarm board to determine that TOC personnel received alarms when CPE did not communicate to the monitoring equipment.	No exceptions noted.
		Inspected the TOC ticket for a selection of alarms received through the NMS to determine that TOC personnel responded to the alarm.	No exceptions noted.

Control Objective 4 – Data Storage and Destruction

Controls provide reasonable assurance that procedures are in place and followed for the secure storage and destruction of sensitive data to protect data relevant to user entities' internal control over financial reporting.

Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
4.1	US Signal has a formalized Data Protection Policy document that defines how data will be securely stored and destroyed. The policy is reviewed and updated annually.	Inspected the Data Protection Policy to determine that formalized policies and procedures were in place to define how data would be securely stored and destroyed.	No exceptions noted.
		Inspected the revision history of the Data Protection Policy to determine that the policy was reviewed and updated on an annual basis.	No exceptions noted.
4.2	Customer data storage is segregated into individual virtual storage repositories so that customers do not have access to other customers' data.	Inspected the virtual storage dashboard and the cloud customer storage diagram to determine that access to customer data was segregated.	No exceptions noted.
4.3	Customers execute a master services agreement with US Signal which defines the data retention and destruction rules for customer data. Upon termination of services, US Signal will return or delete customer data in accordance with the agreement.	Inspected the management console for a selection of data destruction requests from customers to determine that data was destroyed per the terms of the executed master services agreement.	No exceptions noted.
4.4	US Signal performs a quarterly data audit to ensure data destruction procedures are being followed.	Inspected the US Signal Data Protection Policy and Record Management Policy to determine they documented US Signal's data retention and destruction procedures.	No exceptions noted.

Control Objective 4 – Data Storage and Destruction

Controls provide reasonable assurance that procedures are in place and followed for the secure storage and destruction of sensitive data to protect data relevant to user entities' internal control over financial reporting.

Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
		Inspected audit reports for a selection of quarters to determine management performed a quarterly data audit to ensure US Signal's data retention and destruction procedures were being followed.	No exceptions noted.

Control Objective 5 – Logical Access to Production Network and Managed Data Center Elements

Controls provide reasonable assurance that logical access to the US Signal production network and managed data center elements relevant to user entities' internal control over financial reporting is restricted to authorized and appropriate individuals.

Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
5.1	HR personnel or Department Managers submit requests for access to the production network elements to the IT Helpdesk who validate the request was properly authorized and configure access in the production (RADIUS) server.	Inspected the email or IT Helpdesk ticket for a selection of new hires granted access to the production network to determine that the access was approved by HR personnel or the employee's Department Manager	No exceptions noted.
		Inspected the access in the RADIUS server for a selection of new hires granted access to the production network to determine that the access was appropriately granted based on the user's role and as requested.	No exceptions noted.
5.2	Upon employee termination, the IT Helpdesk removes access to US Signal systems after being notified of the termination by HR personnel.	Inspected the termination notification for a selection of terminated employees to determine that HR personnel notified the IT Helpdesk of the termination.	No exceptions noted.
		Inspected the domain user listing for a selection of terminated employees to determine that access was removed.	No exceptions noted.
		Inspected the OMNI listing for a selection of terminated employees to determine that access was removed.	No exceptions noted.
5.3	Remote access to the US Signal internal network is permitted for Active Directory users via VPN connectivity with Duo Security two-factor authentication connectivity.	Inspected Microsoft Duo configurations to determine that two-factor authentication was used by Active Directory users connecting to the network remotely.	No exceptions noted.

Control Objective 5 — Logical Access to Production Network and Managed Data Center Elements

Controls provide reasonable assurance that logical access to the US Signal production network and managed data center elements relevant to user entities' internal control over financial reporting is restricted to authorized and appropriate individuals.

Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
5.4	Access to production network elements is configured to be restricted to specific protocols, ports, and IP addresses.	Inspected the configuration of production network elements to determine that access was configured to be restricted to specific protocols, ports, and IP addresses.	No exceptions noted.
5.5	Access to the individual production network elements and managed CPE is authenticated through a centralized RADIUS server.	Inspected security configurations for production network elements and managed CPE to determine that access to the devices was controlled through a centralized RADIUS server.	No exceptions noted.
5.6	Access to the RADIUS server, which restricts access to the production network elements, is configured to authenticate via Active Directory.	Inspected RADIUS server configurations to determine it was configured to authenticate via Active Directory.	No exceptions noted.
5.7	Network password restrictions are enabled for password length, strength, duration, history, and lockout settings.	Inspected the default password and lockout policies for the US Signal domain to determine that passwords were enabled and enforced password length, strength, duration, history, and account lockout.	No exceptions noted.
5.8	Logging and monitoring of security events and system alerts are enabled on network elements and are configured to log activity to an internal SIEM and the Company's NMS.	Inspected configurations of production network elements for a selection of devices to determine they were configured to log activity to the internal SIEM and NMS.	No exceptions noted.
5.9	Security alerts from the NMS are monitored in real time by the TOC.	Observed TOC personnel to determine they monitored security events in real time through the NMS.	No exceptions noted.

Control Objective 5 – Logical Access to Production Network and Managed Data Center Elements

Controls provide reasonable assurance that logical access to the US Signal production network and managed data center elements relevant to user entities' internal control over financial reporting is restricted to authorized and appropriate individuals.

Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
5.10	Access to manage the virtual components for the managed data center services is restricted through the Management Console, which is configured to authenticate users using LDAP.	Inspected the configuration of the Management Console to determine that it was configured to authenticate users using LDAP.	No exceptions noted.
5.11	Users with the ability to access the vSphere are limited to authorized and appropriate IT personnel based on job responsibilities.	Inspected the access listing for the vSphere to determine that access was limited to appropriate IT personnel based on job responsibilities.	No exceptions noted.
		Corroboratively inquired of the CISO and Director of Cloud Engineering to determine that access to create or modify users was limited to authorized and appropriate IT personnel based on their job responsibilities.	No exceptions noted.
5.12	Privileged access to the network, applications, application databases, secured network drives, and back-end supporting systems is reviewed by management on a quarterly basis to ensure that privileged access is restricted to appropriate users based on their job responsibilities. Any access modifications needed as a result of the review are made by management.	Inspected the privileged access reviews for a selection of quarters to determine that privileged access to the network, applications, application databases, secured network drives, and back-end supporting systems were reviewed to ensure that privileged access was restricted to appropriate users based on their job responsibilities, and any access modifications as a result of the review were made by management, if needed.	No exceptions noted.

Control Objective 5 – Logical Access to Production Network and Managed Data Center Elements

Controls provide reasonable assurance that logical access to the US Signal production network and managed data center elements relevant to user entities' internal control over financial reporting is restricted to authorized and appropriate individuals.

Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
5.13	User access to the network is reviewed on a quarterly basis by management to ensure that access is restricted to appropriate users based on job responsibilities. Any access modifications needed as a result of the review are made by management.	Inspected the network access reviews for a selection of quarters to determine that user access to the network was reviewed by management for appropriateness and any access modifications as a result of the review were made by management, if needed.	No exceptions noted.

Control Objective 6 – Physical Security and Environmental Controls

Controls provide reasonable assurance that physical access to the US Signal data center facility containing the production servers and telecommunication equipment used to deliver the managed data center service is restricted to properly authorized individuals and environmental controls exist to protect these resources.

Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
6.1	Access to the corporate headquarters and data center facilities containing production servers and telecommunications equipment is controlled and restricted by an electronic proximity card or biometric access system.	Observed the proximity card access or biometric access system in place for the corporate headquarters, and each US Signal data center facility, to determine that access to the facility was controlled and restricted from unauthorized access by an electronic proximity card or biometric access system.	No exceptions noted.
6.2	The data center facilities' camera and alarm systems are monitored on an ongoing basis by the TOC. Camera and alarm systems are in place at each data center facility to ensure each location is secured and monitored.	Observed the TOC personnel performing their normal duties to determine that US Signal data center facility's cameras and alarm systems were monitored on an ongoing basis.	No exceptions noted.
		Observed the cameras and security alarm for the corporate headquarters, and each US Signal data center facility, to determine that the data centers were secured and monitored.	No exceptions noted.
6.3	For employees, requests for new access or changes to existing access are submitted to the Facilities Department from HR personnel. For customers and vendors, requests for new access or changes to existing access are submitted to the Facilities Department from the customer's or vendor's designated point of contact. Facilities personnel validates the request and creates the new user's access based on the request.	Inspected the email notification sent to the Facilities Department and a ticket for a selection of employees, customers, and vendors who were granted new facilities access or had a change to their existing facilities access to determine that requests for new access or changes to existing access were authorized prior to access being granted.	No exceptions noted.

Control Objective 6 – Physical Security and Environmental Controls

Controls provide reasonable assurance that physical access to the US Signal data center facility containing the production servers and telecommunication equipment used to deliver the managed data center service is restricted to properly authorized individuals and environmental controls exist to protect these resources.

Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
6.4	When employees leave the organization, HR personnel reclaim the terminated employee's access card and notify the Facilities Department via email or ticket so that physical access privileges, such as biometrics or proximity card, will be revoked.	Inspected the email or ticket notification for a selection of terminated employees to determine that HR personnel had notified facilities to disable or revoke physical access.	No exceptions noted.
		Inspected the facilities' physical access listing for a selection of terminated employees to determine that physical access was revoked.	No exceptions noted.
6.5	When US Signal receives a request for removal of customer access to the data center, a ticket is created to track the removal of physical access.	Inspected customer facilities tickets for a selection of customer removal requests to determine access was removed appropriately and physical access removal was tracked in a ticket.	No exceptions noted.
6.6	Physical access to the corporate headquarters and data center facilities is reviewed on a quarterly basis by management. Any access modifications needed as a result of the review are made by management.	Inspected the physical access reviews for a selection of quarters to determine that physical access to the corporate headquarters and data center facilities was reviewed by management and any access modifications as a result of the review were made by management, if needed.	No exceptions noted.

Control Objective 6 – Physical Security and Environmental Controls

Controls provide reasonable assurance that physical access to the US Signal data center facility containing the production servers and telecommunication equipment used to deliver the managed data center service is restricted to properly authorized individuals and environmental controls exist to protect these resources.

Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
6.7	Fire and smoke detectors, automated clean-agent or pre-action wet fire suppression systems, and hand-held fire extinguishers are in place to protect US Signal data center facilities from fire-related hazards.	For each US Signal data center facility, observed the following operational system components to determine that the facility was protected from fire-related hazards: • Fire and smoke detectors • Automated clean-agent or pre-action wet fire suppression system • Handheld fire extinguishers	No exceptions noted.
6.8	The data center facilities feature dedicated climate control systems to control the temperature and humidity within the facilities.	For each US Signal data center facility, observed operational climate control systems to determine that systems were in place to control the temperature and humidity within the facility.	No exceptions noted.
6.9	UPS units and power generation equipment protect the server and telecommunication equipment from power surges and sudden power outages.	For each US Signal data center facility, observed the operational UPS units and power generation equipment to determine that systems were in place to protect corporate and telecommunication equipment from power surges and sudden power outages.	No exceptions noted.

Control Objective 7 – Logical Security - Internal Systems

Controls provide reasonable assurance that logical access to the US Signal internal systems relevant to user entities' internal control over financial reporting is restricted to authorized individuals and is implemented and maintained according to internal specifications and such individuals are restricted to performing authorized and appropriate actions.

Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
7.1	HR personnel or Department Managers submit requests for new-user access to the domain to the IT Helpdesk through an email or ticket. The IT Helpdesk Analyst validates the request and creates the new user's accounts with the appropriate access based on the user's role and access requested.	Inspected the email or IT Helpdesk ticket for a selection of new hires granted access to the domain to determine that the access was approved by HR personnel or the employee's Department Manager.	No exceptions noted.
		Inspected the access in the US Signal domain for a selection of new hires granted access to the domain to determine that the access was appropriately granted based on the user's role and access requested.	No exceptions noted.
7.2	HR personnel or Department Managers submit requests for new user access to the OMNI application to the IT Helpdesk through an email or ticket. The IT Helpdesk Analyst validates the request and creates or modifies the user's account with the appropriate access based on the user's role and access requested.	Inspected the email or IT Helpdesk ticket for a selection of new hires granted access to the OMNI application to determine that access was approved by HR personnel or the employee's Department Manager.	No exceptions noted.
		Inspected the OMNI application user listing for a selection of new hires granted access to the OMNI application to determine that access was appropriately granted based on the user's role and access requested.	No exceptions noted.
7.3	Upon employee termination, the IT Helpdesk removes access to US Signal systems after being notified of the termination by HR personnel.	Inspected the termination notification for a selection of terminated employees to determine that HR personnel notified the IT Helpdesk of the termination.	No exceptions noted.

Control Objective 7 – Logical Security - Internal Systems

Controls provide reasonable assurance that logical access to the US Signal internal systems relevant to user entities' internal control over financial reporting is restricted to authorized individuals and is implemented and maintained according to internal specifications and such individuals are restricted to performing authorized and appropriate actions.

Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
		Inspected the domain user listing for a selection of terminated employees to determine that access was removed.	No exceptions noted.
		Inspected the OMNI listing for a selection of terminated employees to determine that access was removed.	No exceptions noted.
7.4	In accordance with the US Signal Information Security Policy, users with access to US Signal systems require a uniquely assigned identifiable user ID.	Inspected the Information Security Policy to determine that it documented the requirement for users needing unique user IDs to access US Signal systems.	No exceptions noted.
		Inspected the list of network users for the US Signal domain to determine that users were assigned unique user IDs.	No exceptions noted.
		Inspected the list of OMNI users to determine that users were assigned unique user IDs.	No exceptions noted.
7.5	Network password restrictions are enabled for password length, strength, duration, history, and lockout settings.	Inspected the default password and lockout policies for the US Signal domain to determine that passwords were enabled and enforced password length, strength, duration, history, and account lockout.	No exceptions noted.
7.6	The ability to create or modify users and user access privileges is limited to authorized and appropriate IT personnel based on job responsibilities.	Inspected the listing of users with administrative access to the domain to determine that access was restricted to appropriate IT personnel based on job responsibilities.	No exceptions noted.

Control Objective 7 – Logical Security - Internal Systems

Controls provide reasonable assurance that logical access to the US Signal internal systems relevant to user entities' internal control over financial reporting is restricted to authorized individuals and is implemented and maintained according to internal specifications and such individuals are restricted to performing authorized and appropriate actions.

Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
		Corroboratively inquired of the Director of Technical Operations and CISO to determine that access to create or modify users was limited to authorized and appropriate IT personnel based on their job responsibilities.	No exceptions noted.
7.7	Potential Active Directory security violations, including users gaining administrative access to the system, are logged within the SIEM.	Inspected InsightIDR logs to determine potential Active Directory security violations were logged within the SIEM.	No exceptions noted.
7.8	OMNI password parameters are in place and are set to require minimum length, complexity, expiration, history, and lockout settings.	Inspected the OMNI password parameters to determine that it was configured to enforce minimum length, complexity, expiration, history, and lockout settings.	No exceptions noted.
7.9	Privileged access to the network, applications, application databases, secured network drives, and back-end supporting systems is reviewed by management on a quarterly basis to ensure that privileged access is restricted to appropriate users based on their job responsibilities. Any access modifications needed as a result of the review are made by management.	Inspected the privileged access reviews for a selection of quarters to determine that privileged access to the network, applications, application databases, secured network drives, and back-end supporting systems were reviewed to ensure that privileged access was restricted to appropriate users based on their job responsibilities, and any access modifications as a result of the review were made by management, if needed.	No exceptions noted.

Control Objective 7 – Logical Security - Internal Systems

Controls provide reasonable assurance that logical access to the US Signal internal systems relevant to user entities' internal control over financial reporting is restricted to authorized individuals and is implemented and maintained according to internal specifications and such individuals are restricted to performing authorized and appropriate actions.

Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
7.10	User access to the network is reviewed on a quarterly basis by management to ensure that access is restricted to appropriate users based on job responsibilities. Any access modifications needed as a result of the review are made by management.	Inspected the network access reviews for a selection of quarters to determine that user access to the network was reviewed by management for appropriateness and any access modifications as a result of the review were made by management, if needed.	No exceptions noted.

Control Objective 8 – Corporate Network Security

Controls provide reasonable assurance that corporate connections to the internet or other networks relevant to user entities' internal control over financial reporting are protected from unauthorized access.

Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
8.1	US Signal has firewalls at the perimeter of their network to protect their corporate systems from external threats. These firewalls have been configured to protect the perimeter connection, interconnections with customers' networks, and secure network entry points within the organization.	Inspected a network diagram and firewall configurations to determine that firewalls had been configured to protect the perimeter connection, interconnections with customers' networks, and secure network entry points within the organization.	No exceptions noted.
8.2	Firewalls have been configured to analyze the data and packets that are routed through the network and deny access to unauthorized traffic.	Inspected firewall configurations to determine that firewalls were configured to deny access to unauthorized traffic.	No exceptions noted.
8.3	Firewalls include intrusion prevention features to detect and alert on potential threats. Specific thresholds are defined within the IDS/IPS tools, and a breach of those thresholds automatically sends logs to a log aggregation tool and alerts US Signal of potential threats.	Inspected firewall security settings and the logging tool used by US Signal to determine that firewall performance was monitored.	No exceptions noted.
		Inspected firewall system settings and the logging tool used by US Signal to determine that intrusion prevention would detect and alert system administrators to potential threats.	No exceptions noted.
8.4	If a network component goes offline, an automated alert is sent to the TOC through the NMS application.	Inspected NMS application configurations to determine that it was configured to alert TOC staff in the event that a network component goes offline.	No exceptions noted.

Control Objective 8 – Corporate Network Security

Controls provide reasonable assurance that corporate connections to the internet or other networks relevant to user entities' internal control over financial reporting are protected from unauthorized access.

Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
8.5	US Signal uses WPA2 encryption on wireless network connections, and access is limited to Active Directory users.	Inspected wireless security configurations to determine that WPA2 encryption was used on wireless network connections and that access was restricted to Active Directory users.	No exceptions noted.
8.6	Remote access to the US Signal internal network is permitted for Active Directory users via VPN connectivity with Duo Security two-factor authentication connectivity.	Inspected Microsoft Duo configurations to determine that two-factor authentication was used by Active Directory users connecting to the network remotely.	No exceptions noted.
8.7	Endpoint protection software protects production and email servers, workstations, and network-connected laptops against viruses and other malicious code.	Inspected the antivirus software for a selection of workstations and network-connected laptops to determine that antivirus software had been installed.	No exceptions noted.
		Inspected the antivirus software for a selection of servers to determine that antivirus software had been installed.	No exceptions noted.
8.8	Endpoint protection software is configured to monitor data and traffic on production and email servers, workstations, and network-connected laptops with virus signature definitions that are automatically updated from the vendor.	Inspected the antivirus software configurations to determine that it was configured to monitor data and traffic on production and email servers, workstations, and network-connected laptops with virus signature definitions that are automatically updated from the vendor.	No exceptions noted.
8.9	US Signal has a predefined listing of software that is prohibited from being installed on company laptops and workstations. Software on the predefined listing is automatically uninstalled, and IT is alerted.	Inspected the list of predefined prohibited software to determine that IT had a predefined list in place.	No exceptions noted.

Control Objective 8 – Corporate Network Security

Controls provide reasonable assurance that corporate connections to the internet or other networks relevant to user entities' internal control over financial reporting are protected from unauthorized access.

Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
		Inspected ManageEngine configurations to determine that it was configured to uninstall software on the predefined listing and alert IT.	No exceptions noted.