SOC 2SM Type 2 Report on Security and Availability

Report on Colohouse, L.L.C.'s Description of its Data Center Services System and Suitability of the Design and Operating Effectiveness of its Controls

For the period September 1, 2023
through August 31, 2024

Assurance • Tax • Advisory

C O N T E N T S

Section I: Independent Service Auditor's Report

Section I: Independent Service Auditor's Report

To the Management of Colohouse, L.L.C. c/o Hivelocity
8010 Woodland Center Blvd., Suite 700
Tampa, Florida 33614

Scope

We have examined Colohouse, L.L.C.'s (Colohouse) accompanying description of its Data Center Services System (the "system") titled "Description of Colohouse, L.L.C.'s Data Center Services System" throughout the period September 1, 2023 to August 31, 2024, (description) based on the criteria for a description of a service organization's system set forth in DC Section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance – 2022)* in AICPA, *Description Criteria*, (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period September 1, 2023 to August 31, 2024, to provide reasonable assurance that Colohouse's service commitments and system requirements were achieved based on trust services criteria relevant to Security and Availability (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus – 2022)* in AICPA, *Trust Services Criteria.*

Colohouse uses the following subservice organizations: Digital Realty Data Center Solutions (Digital Realty), fifteenfortyseven Critical Systems Realty (fifteenfortyseven), Equinix, and CyrusOne to provide data center services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Colohouse, to achieve Colohouse's service commitments and system requirements based on the applicable trust services criteria. The description presents Colohouse's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Colohouse's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by 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 complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Colohouse, to achieve Colohouse's service commitments and system requirements based on the applicable trust services criteria. The description presents Colohouse's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Colohouse's controls. Our examination did not include such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Colohouse is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Colohouse's service commitments and system requirements were achieved. Colohouse has provided an assertion titled "Colohouse, L.L.C.'s Assertion over its Data Center Services System" (assertion) about the description and the suitability of design and operating effectiveness of the controls stated therein. Colohouse is responsible for preparing the description and assertion; including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively.
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Evaluating the overall presentation of the description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

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 report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls tested and the nature, timing, and results of those tests are presented in the section of our report titled "Section IV: Weaver and Tidwell, L.L.P.'s Description of Tests of Controls and Results."

Opinion

In our opinion, in all material respects,

a. The description presents Colohouse's Data Center Services System that was designed and implemented throughout the period September 1, 2023 to August 31, 2024 in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period September 1, 2023 to August 31, 2024, to provide reasonable assurance that Colohouse's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the period and if the subservice organizations and user entities applied the complementary controls assumed in the design of Colohouse's controls throughout the period.

c. The controls stated in the description operated effectively throughout the period September 1, 2023 to August 31, 2024, to provide reasonable assurance that Colohouse's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Colohouse's controls operated effectively throughout the period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section IV of our report titled "Weaver and Tidwell, L.L.P.'s Description of Tests of Controls and Results" is intended solely for the information and use of Colohouse; user entities of Colohouse's Data Center Services System during some or all of the period September 1, 2023 through August 31, 2024, business partners of Colohouse's subject to risks arising from interactions with Colohouse's Data Center Services System; practitioners providing services to such user entities and business partners; prospective user entities and business partners; and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties.
- Internal control and its limitations.
- Complementary subservice organization controls and complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

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

Weaver and Tidwell, L.L.P.

WEAVER AND TIDWELL, L.L.P.

Fort Worth, Texas
November 21, 2024

Section II: Management's Assertion

Section II: Management's Assertion

Colohouse, L.L.C.'s Assertion over its Data Center Services System

We have prepared the accompanying description of Colohouse, L.L.C.'s (Colohouse) Data Center Services System (the "system") titled, "Description of Colohouse, L.L.C.'s Data Center Services System" for the period September 1, 2023 through August 31, 2024, (description) based on the criteria for a description of a service organization's system set forth in DC Section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance – 2022)* in AICPA, *Description Criteria* (description criteria). The description is intended to provide report users with information about Colohouse's Data Center Services System that may be useful when assessing the risks arising from interactions with Colohouse's system, particularly information about system controls that Colohouse has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Availability (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus – 2022)* in AICPA, *Trust Services Criteria*.

Colohouse uses the following subservice organizations: Digital Realty Data Center Solutions (Digital Realty), fifteenfortyseven Critical Systems Realty (fifteenfortyseven), Equinix, and CyrusOne to provide data center services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Colohouse, to achieve Colohouse's service commitments and system requirements based on the applicable trust services criteria. The description presents Colohouse's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Colohouse's controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Colohouse, to achieve Colohouse's service commitments and system requirements based on the applicable trust services criteria. The description presents Colohouse's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Colohouse's controls.

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

a. The description presents Colohouse's Data Center Services System that was designed and implemented throughout the period September 1, 2023 to August 31, 2024, in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period September 1, 2023 to August 31, 2024, to provide reasonable assurance that Colohouse's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations and user entities applied the complementary controls assumed in the design of Colohouse's controls throughout that period.

c. The controls stated in the description operated effectively throughout the period September 1, 2023 to August 31, 2024, to provide reasonable assurance that Colohouse's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Colohouse's controls operated effectively throughout that period.

Section III: Description of Colohouse, L.L.C.'s Data Center Services System

Section III: Description of Colohouse, L.L.C.'s Data Center Services System

Purpose and Objective of the Report

This report provides an overview of Colohouse, L.L.C.'s (Colohouse) system of internal control related to their Data Center Services System (the "system") provided to its clients, procedures performed by Colohouse relevant to these services, and Colohouse's complementary service organization and complementary user entity controls. Colohouse's Data Center Services System encompasses all activities that are performed by the system relating to the data center services.

This description has been provided to enable the independent auditors of Colohouse's clientele to plan audits in accordance with authoritative guidance provided by the American Institute of Certified Public Accountants (AICPA) in AU-C Section 402, Audit Considerations Relating to an Entity using a Service Organization. The contents of this report are for the common needs of a broad range of user entities and their auditors and may not include every aspect of the service organization's system that each individual user entity and its auditor may consider important in its own particular environment.

This report focuses on the Security and Availability Categories:

- Security: Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet its objectives.
- Availability: Information and systems are available for operation and use to meet the entity's objectives.

This report does not cover:

a. Services or activities performed by the subservice organizations and
b. Services related to the additional Privacy, Confidentiality, and Processing Integrity criteria.

The control activities were reviewed for the services provided and administered by Colohouse related to its Data Center Services System. This description does not encompass every aspect of Colohouse's activities or services provided to its clients, as certain other activities other than Colohouse, L.L.C.'s data center services are not subject to the control environment at Colohouse.

For purposes of this report, "clients" or "user entities" refer to any institution using Colohouse's services.

Parenthetical references have been included throughout Section III as a cross reference to the applicable controls included in Section IV of this report.

Overview of Operations

Colohouse's headquarters during the testing period were located at 36 NE 2nd Street, Suite 400 Miami, FL 33132 which is also the site of a primary data center location in Miami. There are other corporate and data center supporting functions in designated office locations in Texas, Utah, Colorado, Illinois and New York. Colohouse provides a suite of services as described below:

Data Center Colocation Services

Colohouse provides purpose-built data center facility sites identified in the System Boundaries section below. The sites offer space, power, and cooling, reliability, redundancy, and customization to meet the unique business needs of a wide range of customers spanning across numerous industry verticals. Colohouse data center facilities include the space, power, and cooling system infrastructure for its

customer's information systems. The specific controls, techniques, and procedures of controlling, monitoring, and maintaining critical infrastructure varies based on the specific Subservice Organization.

Critical infrastructure features may include:

- N+1 Generators
- N+1 Uninterruptible Power Supply (UPS)
- N+1 CRAC cooling
- Preventative maintenance contracts
- Fuel re-supply contracts

Physical Security

Colohouse data center sites include the implementation, maintenance, and administration of barriers, point-of-entry access points, physical access control systems and onsite security staff for the safeguard of customer information systems and assets located within the sites. The specific controls, techniques, and procedures of controlling, monitoring, and recording vary based on the specific Subservice Organization.

Physical security features and controls may include:

- Perimeter fencing
- External and internal security lighting
- Reinforced exterior walls
- Control points between exterior and customer equipment.
- Biometric scanners (finger, hand, eye)
- Proximity card readers
- Combination locks
- Key code pads
- 30-day minimum video activity storage and retention
- Security guard stations
- Visitor checking/checkout log, kiosks or stations

Customers may order and implement additional or customized security controls and techniques to meet their needs within their dedicated cabinet or cage environments with Colohouse oversight, review, inspection, and final approval.

Environmental Protection

Colohouse data center sites include the implementation, maintenance, and administration of building codes, environmental health and safety requirements, and critical mechanical and electrical components to maintain industry accepted standards. The specific controls, techniques, and procedures of controlling, monitoring, and maintaining environmental protection features varies based on the specific Subservice Organization.

Environmental protection features and controls may include:

- Building Management System (BMS)
- Fire Detection and Suppression
- Power Management and Backup Power
- HVAC
- Leak Detection Systems
- Regular Scheduled Inspection Rounds

Colocation Service Locations

- Miami, FL – 36 NE 2nd Street, Suite 400 (Digital Realty)
- Latham, NY – 175 Old Loudon Rd (Colohouse)
- Orangeburg, NY – 1 Ramland Road (1547 Critical Systems Realty)
- Colorado Springs, CO – 102 South Tejon Street (Colohouse)
- Philadelphia, PA – 2401 Locust Street (Colohouse)
- Chicago, IL – 725 S. Wells Street (1547 Critical Systems Realty)
- Chicago, IL – 350 E. Cermak Street (Digital Realty)

Connectivity Services

Colohouse takes a carrier-neutral approach to connectivity services and connects to major Carrier Hotel Meet-Me-Rooms (MMRs) and Regional Internet Exchanges in Miami, Atlanta, New York, Chicago, and Colorado Springs through direct carrier connectivity, through Subservice Organization offerings, or cross connect capabilities. This allows for a wide variety of options to meet customer's Internet to provide for their connectivity needs.

Colohouse maintains and operates both IPv4 and IPv6 address space and ASN announcements for Internet routing via BGP. Colohouse offers its own blend of Internet bandwidth to its customers.

Colohouse provided connectivity services are generally provided through 1Gb and 10Gb Ethernet ports at all sites. Certain limited sites utilize and are capable of providing 100Gb Internet connectivity.

Connectivity Service Locations

- Miami, FL – 36 NE 2nd Street, Suite 400 (Digital Realty)
- Latham, NY – 175 Old Loudon Rd (Colohouse)
- Orangeburg, NY – 1 Ramland Road (1547 Critical Systems Realty)
- Colorado Springs, CO – 102 South Tejon Street (Colohouse)
- Philadelphia, PA – 2401 Locust Street (Colohouse)
- Chicago, IL – 725 S. Wells Street (1547 Critical Systems Realty)
- Chicago, IL – 350 E. Cermak Street (Digital Realty)
- Atlanta, GA – 56 Marietta Street (Digital Realty)
- Chandler, AZ – 2335 South Ellis Street (CyrusOne)

Hosting Services

Colohouse offers a wide array of hosting service capabilities, including dedicated servers, website, cPanel, SEO, Virtual Private Servers (VPS), and Managed VPS services. These options meet various customer needs looking for performance, value, and security.

These services offer bundled features that include customization (e.g., CPU, ram, hard disks, raid configurations, bandwidth, IP addresses, and self-management and self-monitoring) capabilities through an online ordering, provisioning, administration and billing platform.

Hosting Service Locations

- Miami, FL – 36 NE 2nd Street, Suite 400 (Digital Realty)
- Latham, NY – 175 Old Loudon Rd (Colohouse)
- Orangeburg, NY – 1 Ramland Road (1547 Critical Systems Realty)
- Colorado Springs, CO – 102 South Tejon Street (Colohouse)
- Philadelphia, PA – 2401 Locust Street (Colohouse)
- Chicago, IL – 725 S. Wells Street (1547 Critical Systems Realty)
- Chicago, IL – 350 E. Cermak Street (Digital Realty)

Cloud Services

Colohouse provides an advanced multi-tenant and dedicated private cloud platform based on VMware technology. The VMware virtualization technology allows customer technical staff a familiar platform capable of running business critical virtual machines with enterprise class scalability, performance, recoverability, failure protection, flexible deployments, workload optimization, and security.

Cloud customer environments can be deployed as full-stack dedicated single-tenant infrastructure for the highest levels of security, dedicated compute multi-tenant infrastructure, or as a fully shared multi-tenant infrastructure. Multi-tenant environments are secured using vendor virtualization hardware segmentation security, vendor network VLAN traffic segmentation, secure IPSec VPNs for remote access to the environment, and Colohouse managed platform administration.

Infrastructure patching is included and managed for underlying server, network, and storage hardware and VMware virtualization software. Hardware firewalls and firewall rule management provide security from external Internet traffic and Layer 2 through Layer 5 OSI model network related threats.

Cloud Service Locations

- Atlanta, GA – 56 Marietta Street (Digital Realty)
- Chandler, AZ – 2335 South Ellis Street (CyrusOne)

Service Commitments and System Requirements

Colohouse designs their processes and procedures related to the system to meet their objectives for its data center services. Those objectives are based on the service commitments that Colohouse makes to user entities, the laws and regulations that govern the provision of their services, and the financial, operational, and compliance requirements that Colohouse has established for the services. The data center hosting services of Colohouse are subject to the relevant regulatory and industry information and data security requirements in which Colohouse operates.

Security and availability commitments to user entities are documented and communicated in service agreements and other customer agreements, sales and marketing documentation, as well as in the description of the service offering provided online. The principal security and availability commitments are standardized and include, but are not limited to, the following:

- Implementing and maintaining physical security systems and controls at its data centers and facilities to protect the confidentiality, integrity, and availability of customer's mission critical information technology equipment and information; including the establishment of safeguards to protect information resources against, theft, abuse, misuse, distortion, or any form of illegal damage.
- Providing reliable and highly available data center environments through the maintenance and continuous monitoring of environmental conditions and systems for adherence to Colohouse's availability service-level commitments.
- Establishing and sustaining incident response, disaster recovery and business continuity programs to respond to and recover from incidents or major service interruptions in a timely manner with minimal damage to customer and company assets, and minimal impact to the services provided.
- Ensuring Colohouse's compliance with the applicable legal, statutory, regulatory requirements, including relevant country-specific regulations.

Colohouse has established operational requirements that support the achievement of the principal service commitments, relevant laws and regulations, and other system requirements. This includes defined company policies and procedures focused on reducing risks related to the achievement of objectives for security and availability; and the implementation of a company-wide systematic approach

for performing annual risk assessments to identify threats and vulnerabilities to objectives and the application of the risk treatment activities to mitigate said risks. It also includes screening procedures during the hiring process; administration of annual formal security awareness training program completion requirements for all personnel; and the use of preventative, detective and responsive control processes and mechanisms to ensure physical and logical access to information and systems is restricted to authorized individuals, as well as to ensure facilities housing customer equipment and support operations are properly provisioned, maintained and monitored to reduce the risks of environmental threats such as power loss, fire, and flooding.

Such requirements are communicated in Colohouse's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired, trained, and managed. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the system.

Subservice Organizations

Colohouse uses the subservice organizations listed below to support certain functions of Colohouse's services:

- Digital Realty Data Center Solutions (Digital Realty)
- fifteenfortyseven Critical Systems Realty (fifteenfortyseven)
- Equinix
- CyrusOne

The subservice organizations provide physical security and environmental data center services that support the entity's infrastructure. Refer to the sub-section titled "Complementary Subservice Organization Controls" for the types of controls Colohouse has assumed that Digital Realty, fifteenfortyseven, Equinix, and CyrusOne have implemented that are applicable to the related criteria identified in the table.

The accompanying description does not include controls performed by the subservice organizations listed above. Weaver and Tidwell, L.L.P.'s (Weaver) examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organizations controls.

Boundaries of the System

The boundaries of Colohouse's data center services are the specific aspects of the Company's infrastructure, software, people, procedures, and data necessary to provide its services. The boundaries of Colohouse's data center services include applications, databases, and infrastructure components that directly support the Colohouse data center services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the Colohouse data center services.

The components that directly support the services provided to customers are described in the subsections below.

Infrastructure

Colohouse's system comprises the physical infrastructure, power, and data connectivity needed to house customer information systems, assets, and data at its facilities; and includes the provision of physical and

environmental security mechanisms to safeguard those customer assets from unauthorized access and environmental threats. A combination of externally supported and wholly purchased application platforms are utilized to support the delivery of data center services. The following table provides a summary of the in-scope infrastructure and information systems:

Primary Infrastructure	
Hardware	**Purpose**
Automatic Transfer Switches ("ATS")	Monitors connection to power supply and activates load transfer to generator if an interruption occurs.
Uninterrupted Power Supplies ("UPS")	Provides emergency backup power prior to going on generator - ensures no interruption in power.
Power Distribution Units ("PDU")	Distributes power to customer space and monitors usage.
Generators	Provide power to the data center in a loss of utility power.
Air Conditioning and Cooling ("HVAC")	Provides proper cooling and humidity to the data center and monitors levels.
Fire Detection & Suppression System	Protects against fires.
Physical Access Control Systems (various platforms – varies by region/location)	Access control hardware and software used to regulate access to data center facilities.
Closed circuit television ("CCTV") and security cameras system (various platforms – varies by location)	Surveillance camera system hardware and software used for security monitoring of data centers 24 hours per day; CCTV cameras are positioned throughout the data centers to monitor and track the activity of any person while inside and outside of the data centers.
Routers, Switches, Firewalls, VPN Gateways	Managed network devices and systems utilized to route traffic for Colohouse's network; restrict and filter traffic, and VPN gateway network devices used to facilitate secure connectivity for data centers (site-to-site) and end users (point-to-point).
Servers	Supports the customer facing web applications. Web-based applications used by clients to manage their access control lists including access change requests and visitor access requests to data center; place orders for data center products and schedule services; and view order statuses, access reports, account information, and review invoices.
Storage Systems	Disk storage devices used to present files and directories to local host and to hosts over the network.
Cloud Platforms	Internal systems and Colohouse cloud services.

Software

Software consists of the programs and software that support the Colohouse System, including software used to build, support, secure, maintain, and monitor the Colohouse System. The following table provides a summary of the software utilized to support the Colohouse System:

Primary Software		
Software	**Operating System**	**Purpose**
Service Delivery Systems (multiple systems – varies by service)	Linux	Provisioning, asset management, service tracking, and reporting management systems for network, hosting and colocation services.
Commercial Software Vendors (various vendors)	Windows / Linux	Provides features and functionality for the delivery of hosting and cloud services capabilities.
Kayako and ServiceNow Ticketing Systems	SaaS	Ticketing system used to record, track, and monitor external and internal reported incidents, requests and alerts.
OpsGenie	SaaS	Escalation pager application used to assist with emergency notifications and response regarding changes within major infrastructure and service level agreements ("SLA") requirements.
GitLab	CentOS 6	Development tracking software for internal systems.
Device and Network Monitoring Systems (multiple systems – varies by service)	Linux	Infrastructure and network monitoring software for Colohouse datacenter and customer services.
Salesforce	SaaS	Customer account, contract and service order management, and customer notifications.
Ordering and Billing Systems (multiple systems – varies by service)	Linux	Provides ordering and billing system for colocation, hosting, and cloud services.
Corporate IT Systems (multiple systems)	SaaS	Provides communication, collaboration, and security internally and externally.

People

Colohouse manages and secures the Colohouse System via separate departments. The responsibilities of these departments are defined as follows:

People	
Group/Role Name	**Function**
Executive Management	Responsible for providing overall guidance and oversight of Colohouse's products and services.
Finance	Responsible for managing, controlling and accounting for all company finances, cash-flow and financial reporting, including financial statements.
Human Resources	Responsible for managing employee-related issues such as hiring, training, development, compensation, benefits, communication, and administration.
Product and Technology	Responsible for creating standard architectures, developing new services, and managing existing services offered to customers and internal systems of Colohouse.
Marketing and Sales	Responsible for promoting and marketing the services of Colohouse to potential customers and clients.

People	
Group/Role Name	**Function**
Technical Support Team/Service Operations	Responsible for the resolution of all technical requests made by customers to the satisfaction of the customer. Responsible for delivering a responsive system that fully complies with the functional specification. Verifies that the system complies with the functional specification through functional testing procedures. Responsible for effective provisioning, installation/configuration, operation, and maintenance of systems.
Account Management	Serves customers by providing product, service and support information and guidance. Advocates for the customer in resolving product and service issues.

Policies and Procedures

Procedures include the automated and manual procedures involved in the operation of Colohouse System. Procedures are developed and documented by the respective teams for a variety of processes, including those relating to product management, engineering, technical operations, security, and HR. These procedures are drafted in alignment with the overall information security policies and are updated and approved as necessary for changes in the business, but no less than annually.

Elements of the Control Environment, Risk Assessment, Communication, and Monitoring

A. Control Environment
B. Communication
C. Risk Management
D. Monitoring
E. Logical and Physical Access
F. System Operations
G. Change Management
H. Risk Mitigation
I. Availability

A. Control Environment

Control Environment

The control environment is the foundation for other areas of internal control. As such, the control environment sets the tone for the organization and reflects the overall attitude, awareness, and actions of Colohouse management and other stakeholders. Management of Colohouse emphasizes the importance of controls and ethical behavior throughout the organization. The parenthetical references identify key control activities that are mapped against the required Trust Services Criteria.

Integrity and Ethical Values

The effectiveness of controls is dependent upon the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Colohouse's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Colohouse's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

Management's Philosophy and Operating Style

Colohouse's management is committed to maintaining the highest levels of ethics and integrity. Management endeavors to foster this culture by promoting cooperation, coordination, communication,

and alignment of interests within and among Colohouse employees, clientele, and other involved parties. Annually, Colohouse security, availability, and confidentiality policies are reviewed and approved by senior management. These policies are made available to employees through the corporate intranet platform. Changes to policy documentation are communicated to employees through a combination of verbal announcements during meetings, e-mail announcements and publication to the corporate intranet and to customers through e-mail and/or updated website content. In addition, any changes that may affect customers, their security, availability, and confidentiality obligations, or Colohouse's commitments are communicated internally and externally through e-mail. Each department is responsible for creating a control-conscious environment. Senior management reviews the policies on a department-by-department basis and sets overall companywide policy.

Organizational Structure and Assignment of Authority and Responsibilities

The Chief Executive Officer ("CEO") of Colohouse is appointed by the Board of Managers of COLO Holdings, LLC to oversee daily operations and lead the management team. Supporting the CEO are the following functional departments that manage and perform the daily operations of Colohouse: finance, legal, human resources, sales, marketing, operations, technology, and product development. These core competencies have been established to provide full capabilities to serve clients. Colohouse's CEO exercises oversight of the development and performance of internal control and company performance and objectives. **(015)**

Human Resources

An employee handbook and code of conduct are documented to communicate workforce conduct standards and enforcement procedures. **(013)** Personnel are required to read and accept the code of conduct, the employee handbook, and the statement of confidentiality at the time of hire. Background checks are also performed for all new employees. **(014)** Colohouse follows best practice hiring and training procedures to ensure that the personnel responsible have requisite qualifications and skills to fulfill their responsibilities. **(022)** Colohouse provides annual security training for employees and the results are monitored by management in order to track compliance with training requirements. **(019)**

Written job descriptions exist for all key firm personnel and background checks are performed on all new employees**. (012)** Roles and responsibilities are defined in written job descriptions and communicated to personnel through the company SharePoint site. **(018)**

Colohouse has established an organizational structure, reporting lines, authorities, and responsibilities as part of its business planning process and risk assessment processes. Colohouse revises these when necessary to help meet changing commitments and requirements. **(017)**

Organizational and information security policies and procedures are documented for supporting the functioning of controls and processes and made available to its personnel through the company SharePoint site. **(025)** Colohouse has developed an IT policies and procedures manuals which documents the information that employees need related to security and availability in order to carry out their responsibilities. Colohouse's data center management is responsible for maintaining and updating the IT policies and procedures documents and communicating it to internal personnel as and when required. **(028)**

Operational and security policies are reviewed and updated, if necessary, on an annual basis**. (037)**

Senior Management meets on at least a quarterly basis to discuss operating issues, incidents, and provide oversight of Colohouse's internal control environment. **(001)** Executive management has established proper segregations of duties for key job functions and roles within the organization. **(020)**

B. Communication

Colohouse regularly informs and communicates to internal users about the systems, controls, policies and procedures, through a variety of methods such as periodic e-mails to users and through the operations and incident reporting procedures. **(029)**

A privacy notice is posted on Colohouse's website. The privacy notice describes the entity's privacy commitments. **(034)**

Service commitments are communicated to customers through the terms and conditions made available on the company website. **(031)** Customer responsibilities are outlined and communicated through defined service level agreements (SLA), master service agreements (MSA) and/or the entity website. **(032)**

Documented escalation procedures for reporting failures, incidents, concerns, and other complaints are in place and shared with external parties and made available to employees through the company intranet. **(033)**

Colohouse has developed a strategic plan that identifies key strategic objectives, organization goals, and key performance indicators that allow the organization to establish plans to meet these goals as well as to identify and assess risks that threaten the achievement of these objectives. **(035)**

C. Risk Management

Organizational Risk Management

Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating, and addressing risks and defining specified risk tolerances. **(073)** Colohouse performs a risk assessment of critical systems and operations to monitor the operational, financial, and compliance (including fraud assessment) risks and their effect on system security. Action plans are developed, if required, to mitigate the risks identified due to these changes. **(036)** A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements. **(074)**

Vendor Risk Management

A vendor risk assessment is performed on an annual basis which includes reviewing the activities performed by third parties. **(021)**

D. Monitoring

Monitoring Activities

Senior Management meets on at least a quarterly basis to discuss operating issues, incidents, and provide oversight of Colohouse's internal control environment. **(001)**

Enterprise monitoring software is utilized to notify personnel when predefined thresholds are exceeded on production systems. **(003)** Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. **(027)** Monitoring software and network hardware (i.e., firewalls) are in place to monitor system security, vulnerabilities, and changes that are made to the system. **(063)**

Environmental systems are monitored and issues related to environmental equipment are documented and resolved timely by network operations center ("NOC") personnel. **(064)**

Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities. **(042)**

E. Logical Access and Physical Access

Logical Access

Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring. **(048)**

The data center systems are configured to enforce password requirements that include at least one, if not all, of the following requirements: minimum password length, password complexity, password change requirements. **(047)** VPN user access is restricted via role-based security privileges defined within the access control system. VPN users are authenticated via username, password, and multifactor authentication. **(046)**

VPN and SSL encryption technologies are used for defined points of connectivity. **(057)** Transmission of digital output beyond the boundary of the system is encrypted. **(059)** Network address translation (NAT) functionality is utilized to manage internal IP addresses. **(056)**

Client access lists are configured based on the access control list submitted during the onboarding process. **(045)**

Physical Access

Policies and procedures are in place to guide personnel in physical security activities. **(052)**

The physical access to the data center is restricted to the authorized individuals using a card key to unlock the door. Access to the data center is limited to authorized Colohouse employees based on their roles and responsibilities. Access to the data center is approved by data center management. In addition, modification and removal of access is requested by a manager and approved by data center management. **(049)**

A manned reception desk is in place to monitor and control access to the entrance of the office facility during standard business hours. **(053)** A badge access system controls access to and within the office facility. The sharing of access badges and tailgating are prohibited. **(054)**

User access to the badge access system is reviewed on an annual basis. **(055)**

Visitors and contractors are required to sign in and are escorted by authorized personnel when accessing the facility. **(044)** Visitors to the facility are required to sign a visitor log upon arrival and must be signed in by an authorized workforce member before a single-day visitor badge that identifies them as an authorized visitor can be issued. Visitor badges are issued for identification purposes only and do not permit access to any secured areas of the facility. All visitors must be escorted by a workforce member when visiting facilities where sensitive system and system components are maintained and operated. Visitors must return their visitor badge at the end of their visit to the security desk. **(050)**

Surveillance cameras are located at strategic locations within all data centers to monitor access into the facility and data center floor space as a deterrent to unauthorized access. **(051)**

F. System Operations

Documented incident response policies and procedures are in place to guide personnel in the event of an incident. **(066)** Documented escalation procedures for reporting failures, incidents, concerns, and

other complaints are in place and shared with external parties and made available to employees through the company intranet. **(033)**

Vulnerability scans are performed annually on the environment to identify control gaps and vulnerabilities, and remedial actions are taken where necessary. **(039)**

Antivirus software is installed on workstations and configured to conduct periodic scans to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software. The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available. **(061)**

Problems and incidents are documented, tracked, and resolved in a timely manner. **(038)**

A business continuity plan and disaster recovery plan are in place to guide personnel in the decisions, responsibilities and requirements following disruptions to services and operations. The recovery plans identify, select, and define risk mitigation activities for risks arising from potential business disruptions. **(005)**

Disaster recovery and backup restoration testing is performed on an annual basis, test results are reviewed and contingency plans are adjusted as needed. **(077)**

G. Change Management

Documented change control policies and procedures are in place to guide personnel in handling system changes to be in accordance with the change management process. **(060)** Documented change control policies and procedures are in place to guide personnel in implementing changes in an emergency situation. **(072)**

All changes to the Colohouse systems must be logged and implemented as per the documented change management policies. All changes, are initiated by a request, authorized for implementation, tested (if needed) and approved by clients and Colohouse management prior to commencing any work in the data center. **(067)**

System change requests are documented and tracked in a ticketing system, changes are approved by management and tested prior to implementation. Types of testing performed depend on the nature of the change. **(070)**

Access to the data center for the purposes of implementing changes is limited to authorized Colohouse employees and client and vendors who are authorized to access the data center floor space. **(068)**

H. Risk Mitigation

Vendor Risk Management

Management has defined a third-party vendor risk management process that specifies the process for evaluating third-party risks based on identified threats and the specified tolerances. **(076)**

Colohouse has developed a data center management policy and plan that assesses and manages risks associated with vendors and business partners. **(075)**

A vendor risk assessment is performed on an annual basis which includes reviewing the activities performed by third parties. **(021)**

I. Availability

Colohouse has a process in place to ensure scheduled maintenance and other data center changes or updates are documented and authorized to ensure minimal impact to customers. Preventative maintenance is performed periodically on all data center environmental control systems. **(002)**

Enterprise monitoring software is utilized to notify personnel when predefined thresholds are exceeded on production systems. **(003)**

The following environmental controls exist and are adequately maintained to ensure protection of the data centers:

a. HVAC & dehumidifiers
b. Uninterruptible Power Supply
c. Power Distribution Units
d. Adequate lighting in data center
e. Fire suppression
f. Generators **(004)**

Production equipment within the colocation areas of the data center facilities is placed on racks to protect infrastructure from localized flooding. **(006)** The data center facilities are equipped with leak detection systems to detect water in the event of a flood or water leakage**. (008)**

Data center facilities are equipped with raised flooring to elevate equipment and help facilitate cooling. **(007)**

Disaster recovery and backup restoration testing is performed on an annual basis, test results are reviewed and contingency plans are adjusted as needed. **(077)**

Significant Changes During the Period

There were no significant changes that are likely to affect report users' understanding of how the in-scope system is used to provide the service during the period September 1, 2023, to August 31, 2024.

Identified System Incidents

No system incidents were identified during the period September 1, 2023, to August 31, 2024, that resulted in a significant impairment of Colohouse's ability to achieve its service commitments and system requirements related to its Colohouse System, during the period of September 1, 2023, to August 31, 2024, that require disclosure.

Complementary Subservice Organizations Controls

Colohouse's controls are designed with the assumption that subservice organizations will have implemented complementary subservice organization controls that are necessary to achieve the prescribed criteria. Subservice organization controls are implemented by the subservice organization and are necessary to achieve the criteria related to security, as stated in management's description of the service organization's system. The risks that management identifies also include the risk that such controls were not implemented by subservice organizations or that those controls were not operating effectively.

Complementary Subservice Organization Control (CSOCs)	Related Criteria
Digital Realty, fifteenfortyseven, Equinix, and CyrusOne	
The subservice organization has implemented appropriate environmental controls including those preventing unauthorized physical access to sensitive data and equipment.	CC6.2, CC6.4, CC6.5
The subservice organization has implemented controls ensuring incidents, or outages are resolved in a timely manner.	CC7.2, CC7.3, CC7.4, A1.2
The subservice organization has implemented controls to maintain, monitor, and test recovery procedures in order to meet availability commitments.	A1.1, A1.2, A1.3
The subservice organization has implemented controls to monitor third-party, and vendor compliance with security commitments.	CC9.2
The subservice organization has controls in place to appropriately perform change management functions on hosting infrastructure.	CC8.1
The subservice organization has implemented controls in place to ensure geo-redundancy is operating.	A1.1

Complementary User Entity Controls

Management is responsible for identifying the risks that threaten achievement of the criteria stated in management's description of the service organization's system. A service organization's controls may be designed with the assumption that user entities will have implemented complementary user entity controls that are necessary to achieve the prescribed criteria.

Colohouse's controls related to the Colohouse system cover only a portion of overall internal control for each user entity of Colohouse. It is not feasible for the prescribed criteria to be achieved solely by Colohouse. Therefore, each user entity's internal control environment should be evaluated in conjunction with Colohouse's controls described below, taking into account the related complementary user entity controls identified under each prescribed criterion, where applicable. In order for user entities to rely on the controls reported on herein, each user entity must evaluate its own internal control to determine whether the identified complementary user entity controls have been implemented and are operating effectively.

Complementary User Entity Controls (CUECs)	Related Criteria
User entities monitor security violations and report incidents to Colohouse as required, on a timely basis.	CC2.3, CC7.2
User entities should ensure system access is appropriately restricted to authorized users.	CC6.1, CC6.2, CC6.3
User entities should ensure access changes are communicated to Colohouse on a timely basis.	CC6.1, CC6.2, CC6.3
User entities should monitor user access to ensure that only authorized users maintain active access privileges.	CC6.1, CC6.2, CC6.3
User entities should ensure that appropriate controls have been implemented to ensure network and perimeter security controls have been implemented to protect against threats from sources outside the system boundaries.	CC6.6

Complementary User Entity Controls (CUECs)	Related Criteria
User entities should ensure that appropriate controls have been implemented to ensure the transmission, movement, and removal of information to authorized internal and external users and processes is appropriately restricted.	CC6.7
User entities should ensure that appropriate controls have been implemented to ensure the prevention and detection of unauthorized or malicious software is identified.	CC6.8

The list of complementary user organization control considerations presented above does not represent a comprehensive list of all the controls that should be deployed by user organizations. Other controls may be required at the user organization in order to achieve adequate internal control.

Section IV: Weaver and Tidwell, L.L.P.'s Description of Tests of Controls and Results

Section IV: Weaver and Tidwell, L.L.P.'s Description of Tests of Controls and Results

Overview of Description of Tests of Controls and Results

This section of the report is intended to provide interested parties as listed in and limited by Section I of this report with sufficient information to understand the following processes relative to certain aspects of Colohouse's environment.

Our examination was restricted to the description of the system, criteria and the related control procedures specified in Section III by Colohouse management and was not extended to procedures described elsewhere in this report but not listed, or to procedures that may be in effect at the user entities or other service providers utilized by the user entities.

The examination was restricted to the Trust Services Criteria over Security and Availability of Colohouse's Data Center Services System for user entities as listed and, accordingly, do not extend to procedures in effect at user entities.

It is each interested party's responsibility to evaluate this information in relation to internal control policies and procedures in place at the user entities, to obtain an understanding of the internal control policies and procedures and assess control risk. User entities and Colohouse's portions of the controls must be evaluated together. If effective user entities internal control policies and procedures are not in place, Colohouse's internal control policies and procedures may not compensate for such weaknesses.

Our examination included inquiry of appropriate Colohouse management, supervisory and staff personnel; inspection of documents and records, observation of activities and operations; and tests of controls surrounding and provided by Colohouse over their Data Center Services System.

Our tests of controls were performed for the period September 1, 2023 through August 31, 2024 and were applied to the specified Security and Availability criteria.

Trust Services Categories and Criteria, Controls, Testing and Results of Testing

In selecting particular tests of the operational effectiveness of controls, we considered (a) the nature of the items being tested, (b) the types of available evidential matter, (c) the expected efficiency and effectiveness of the test.

In addition, as required by paragraph .36 of AT-C Section 205, Assertion-Based Examination Engagements (AICPA, Professional Standards), when using information produced (or provided) by the service organization/entities (IPE), 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.

The tables on the following pages describe the control activities to achieve the applicable trust services criteria as specified by Colohouse. The control activities to achieve the criteria are the responsibility of Colohouse. The "Test of Operating Effectiveness" and the "Results" are the responsibility of Weaver.

Description of Control Activities, Tests, Results of Tests, and Criteria Mapping

The table below represents the control activities, auditor's test of controls, auditor's results of tests and a control to criteria mapping.

Description of Control Activities, Tests, Results of Tests, and Criteria Mapping				
Control Number	**Criteria Mapping**	**Control Activity**	**Test of Operating Effectiveness**	**Results**
Controls				
001	CC1.2; CC4.1; CC4.2; CC7.3; CC7.4; A1.1	Senior Management meets on at least a quarterly basis to discuss operating issues, incidents, and provide oversight of Colohouse's internal control environment.	For a sample of quarters, inspected meeting documentation to verify management met on at least a quarterly basis to discuss operating issues, incidents, and provide oversight of the internal control environment.	No exceptions noted.
002	A1.1; A1.2; A1.3	Colohouse has a process in place to ensure scheduled maintenance and other data center changes or updates are documented and authorized to ensure minimal impact to customers. Preventative maintenance is performed periodically on all data center environmental control systems.	Inspected the preventative maintenance schedule and maintenance documentation to verify a process for scheduled maintenance to be performed was in place, and to verify preventative maintenance was performed on data center environmental control systems.	No exceptions noted.
003	CC4.1; CC4.2; A1.1; A1.2	Enterprise monitoring software is utilized to notify personnel when predefined thresholds are exceeded on production systems.	Inspected the monitoring software configurations for each in-scope data center to verify enterprise monitoring software was configured to notify personnel when predefined thresholds were exceeded on production systems.	No exceptions noted.

Description of Control Activities, Tests, Results of Tests, and Criteria Mapping				
Control Number	**Criteria Mapping**	**Control Activity**	**Test of Operating Effectiveness**	**Results**
004	A1.1; A1.2	The following environmental controls exist and are adequately maintained to ensure protection of the data centers: a. HVAC & dehumidifiers b. Uninterruptible Power Supply c. Power Distribution Units d. Adequate lighting in data center e. Fire suppression f. Generators	Performed a live walkthrough of all in-scope data centers to verify environmental protections were installed and included the following: a. HVAC & dehumidifiers b. Uninterruptible Power Supply c. Power Distribution Units d. Adequate lighting in data center e. Fire suppression f. Generators	No exceptions noted.
005	CC7.5; CC9.1; A1.2; A1.3	A business continuity plan and disaster recovery plan are in place to guide personnel in the decisions, responsibilities and requirements following disruptions to services and operations. The recovery plans identify, select, and define risk mitigation activities for risks arising from potential business disruptions.	Inspected the business continuity and disaster recovery plan to verify a plan was in place, and defined procedures to guide personnel in the decisions, responsibilities and requirements following disruptions to services and operations.	No exceptions noted.
006	A1.2	Production equipment within the colocation areas of the data center facilities is placed on racks to protect infrastructure from localized flooding.	Performed a live walkthrough of all in-scope data centers to verify production equipment within the colocation areas of the data center facilities was placed on racks to protect infrastructure from localized flooding.	No exceptions noted.
007	A1.2	Data center facilities are equipped with raised flooring to elevate equipment and help facilitate cooling.	Performed a live walkthrough of all in-scope data centers to verify data center facilities were equipped with raised flooring to elevate equipment and help facilitate cooling.	No exceptions noted.
008	A1.2	The data center facilities are equipped with leak detection systems to detect water in the event of a flood or water leakage.	Performed a live walkthrough of all in-scope data centers to verify data center facilities were equipped with leak detection systems to detect water in the event of a flood or water leakage.	No exceptions noted.

Description of Control Activities, Tests, Results of Tests, and Criteria Mapping				
Control Number	**Criteria Mapping**	**Control Activity**	**Test of Operating Effectiveness**	**Results**
012	CC1.3; CC1.4; CC1.5; CC2.2	Written job descriptions exist for all key firm personnel and background checks are performed on all new employees.	For a sample of job roles, inspected job description documentation to verify written job descriptions existed for key firm personnel.	No exceptions noted.
			For a sample of employees hired during the period, inspected background check documentation to verify background checks were performed on new employees.	No exceptions noted.
013	CC1.1; CC1.4; CC1.5; CC2.2	An employee handbook and code of conduct are documented to communicate workforce conduct standards and enforcement procedures.	Inspected the employee handbook to verify that an employee handbook and code of conduct were documented, and verify the document defined workforce conduct standards and enforcement procedures.	No exceptions noted.
014	CC1.1; CC1.4; CC1.5; CC2.2	Personnel are required to read and accept the code of conduct, the employee handbook, and the statement of confidentiality at the time of hire. Background checks are also performed for all new employees.	Inspected the Colohouse Employee Handbook to verify the code of conduct and statement of confidentiality were defined.	No exceptions noted.
			For a sample of employees hired during the period, inspected signed acknowledgements to verify new hires were required to acknowledge the code of conduct, employee handbook, and statement of confidentiality.	No exceptions noted.
			For a sample of employees hired during the period, inspected background check documentation to verify background checks were performed on new employees.	No exceptions noted.

Description of Control Activities, Tests, Results of Tests, and Criteria Mapping				
Control Number	**Criteria Mapping**	**Control Activity**	**Test of Operating Effectiveness**	**Results**
015	CC1.2	Colohouse's CEO exercises oversight of the development and performance of internal control and company performance and objectives.	Inspected the Chief Executive Officer written job description to verify responsibilities for oversight of the development and performance of internal controls and company performance objectives were defined.	No exceptions noted.
017	CC1.2; CC1.3; CC1.5	Colohouse has established an organizational structure, reporting lines, authorities, and responsibilities as part of its business planning process and risk assessment processes. Colohouse revises these when necessary to help meet changing commitments and requirements.	Inspected the corporate organizational chart to verify the organization chart established organizational structure, reporting lines, authorities, and responsibilities.	No exceptions noted.
018	CC1.3; CC1.4; CC1.5; CC2.2	Roles and responsibilities are defined in written job descriptions and communicated to personnel through the company SharePoint site.	Obtained and reviewed a sample of written job descriptions to ensure roles and responsibilities are defined. In addition, obtained communications of job roles to employees.	No exceptions noted.
019	CC1.1; CC1.3; CC1.4; CC1.5; CC2.2; CC5.3	Colohouse provides annual security training for employees and the results are monitored by management in order to track compliance with training requirements.	For a sample of employees who were active during the period, inspected training documentation to verify that annual security training was completed, and verify that the results were monitored by management.	No exceptions noted.
020	CC1.2	Executive management has established proper segregations of duties for key job functions and roles within the organization.	Inspected the corporate organization chart and a sample of job descriptions to verify segregation of duties for key job functions and roles within the organization were defined.	No exceptions noted.
021	CC1.3; CC2.1; CC3.2; CC3.4; CC4.1; CC9.2; A1.2	A vendor risk assessment is performed on an annual basis which includes reviewing the activities performed by third parties.	Inspected the vendor risk assessment to verify that a vendor risk assessment was performed on an annual basis which included reviewing the activities performed by third parties.	No exceptions noted.

Description of Control Activities, Tests, Results of Tests, and Criteria Mapping				
Control Number	**Criteria Mapping**	**Control Activity**	**Test of Operating Effectiveness**	**Results**
022	CC1.1; CC1.4	Colohouse follows best practice hiring and training procedures to ensure that the personnel responsible have requisite qualifications and skills to fulfill their responsibilities.	Inspected the New Hire & Promotion Procedures to verify that hiring and training procedures were in place and defined requirements to ensure that new hire personnel have requisite qualifications and skills to fulfill their responsibilities.	No exceptions noted.
025	CC1.1; CC2.1; CC2.2; CC5.1; CC5.2; CC5.3	Organizational and information security policies and procedures are documented for supporting the functioning of controls and processes and made available to its personnel through the company SharePoint site.	Inspected the Colohouse Corporate Information Security Policy and internal SharePoint site to verify organizational and security policies were documented and made available to its personnel through the company SharePoint site.	No exceptions noted.
027	CC4.1; CC4.2; CC6.6; CC6.7; CC6.8; CC7.1; CC7.2	Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	Inspected the monitoring software configurations for each in-scope data center to verify enterprise monitoring software was configured to evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No exceptions noted.
028	CC1.1; CC2.1; CC2.2; CC5.1; CC5.2; CC5.3	Colohouse has developed an IT policies and procedures manuals which documents the information that employees need related to security and availability in order to carry out their responsibilities. Colohouse's data center management is responsible for maintaining and updating the IT policies and procedures documents and communicating it to internal personnel as and when required.	Inspected the Corporate Information Security Policy to verify information that employees need related to security and availability in order to carry out their responsibilities was defined.	No exceptions noted.

Description of Control Activities, Tests, Results of Tests, and Criteria Mapping				
Control Number	**Criteria Mapping**	**Control Activity**	**Test of Operating Effectiveness**	**Results**
029	CC2.2	Colohouse regularly informs and communicates to internal users about the systems, controls, policies and procedures, through a variety of methods such as periodic e-mails to users and through the operations and incident reporting procedures.	Inspected meeting and email documentation to verify management communicated information regarding systems, controls, and policies and procedures to internal employees.	No exceptions noted.
031	CC2.3	Service commitments are communicated to customers through the terms and conditions made available on the company website.	Inspected the terms and conditions to verify the service commitments were defined and made available on the public company website.	No exceptions noted.
032	CC2.3	Customer responsibilities are outlined and communicated through defined service level agreements (SLA), master service agreements (MSA) and/or the entity website.	Inspected the Colohouse public website to verify customer responsibilities were communicated through defined service level agreements (SLA), master service agreements (MSA) available on the entity's website.	No exceptions noted.
033	CC2.2; CC2.3; CC5.3; CC7.1; CC7.2; CC7.4	Documented escalation procedures for reporting failures, incidents, concerns, and other complaints are in place and shared with external parties and made available to employees through the company intranet.	Inspected the internal escalation procedures and public company website to verify documented escalation procedures for reporting incidents are made available to employees and external parties.	No exceptions noted.
034	CC2.3	A privacy notice is posted on Colohouse's website. The privacy notice describes the entity's privacy commitments.	Inspected the Colohouse public website to verify a privacy notice was made available, and verify the notice described the entity's privacy commitments.	No exceptions noted.

Description of Control Activities, Tests, Results of Tests, and Criteria Mapping				
Control Number	**Criteria Mapping**	**Control Activity**	**Test of Operating Effectiveness**	**Results**
035	CC2.1; CC3.1; CC3.2; CC5.1; CC5.2	Colohouse has developed a strategic plan that identifies key strategic objectives, organization goals, and key performance indicators that allow the organization to establish plans to meet these goals as well as to identify and assess risks that threaten the achievement of these objectives.	Inspected Colohouse strategic planning documentation to verify that Colohouse developed a strategic plan that identified key strategic objectives, organization goals, and key performance indicators.	No exceptions noted.
036	CC2.1; CC3.1; CC3.2; CC3.3; CC3.4; CC4.1; CC4.2; CC5.1; CC9.1	Colohouse performs a risk assessment of critical systems and operations to monitor the operational, financial, and compliance (including fraud assessment) risks and their effect on system security. Action plans are developed, if required, to mitigate the risks identified due to these changes.	Inspected risk assessment documentation to verify management performed an annual risk assessment of critical systems and operations and identified risks relevant to operations, finance, compliance, and fraud. Additionally, remediation plans were developed when required.	No exceptions noted.
037	CC1.1; CC2.1; CC5.1; CC5.2; CC5.3	Operational and security policies are reviewed and updated, if necessary, on an annual basis.	Inspected organizational policies to verify operational and security policies were reviewed on an annual basis.	No exceptions noted.
038	CC4.2; CC6.6; CC6.7; CC6.8; CC7.3; CC7.4; CC7.5	Problems and incidents are documented, tracked, and resolved in a timely manner.	Inspected incident response policies and procedures and inquired with the SVP Technical Operations to verify that no security incidents occurred during the examination period.	No occurrences to test.
039	CC4.1; CC6.7; CC6.8; CC7.1	Vulnerability scans are performed annually on the environment to identify control gaps and vulnerabilities, and remedial actions are taken where necessary.	Inspected vulnerability scan results to verify an annual vulnerability scan was performed on the Colohouse Cloud environment to identify control gaps and vulnerabilities.	No exceptions noted.

Description of Control Activities, Tests, Results of Tests, and Criteria Mapping				
Control Number	**Criteria Mapping**	**Control Activity**	**Test of Operating Effectiveness**	**Results**
042	CC1.3; CC2.2; CC4.1; CC4.2; CC5.1; CC5.2; CC5.3	Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities.	Through inquiry with data center management and inspection of internal policies and plans, determined that performance of the internal controls implemented within the environment were assigned to appropriate process owners and operational personnel based on roles and responsibilities.	No exceptions noted.
044	CC6.4	Visitors and contractors are required to sign in and are escorted by authorized personnel when accessing the facility.	Performed a live walkthrough of all in-scope data centers to verify visitors and contractors are required to sign in and are escorted by authorized personnel when accessing the facility.	No exceptions noted.
045	CC6.1; CC6.2; CC6.3; CC6.5; CC6.7; CC6.8	Client access lists are configured based on the access control list submitted during the onboarding process.	Obtained the most recent data center access documentation and verified that client access is configured and is reviewed by the client and Colohouse personnel to properly reflect external (i.e. client) users' access levels and terminations.	No exceptions noted.
046	CC6.1; CC6.2; CC6.3; CC6.6	VPN user access is restricted via role-based security privileges defined within the access control system. VPN users are authenticated via username, password, and multifactor authentication.	Inspected the VPN user listing to determine that VPN user access was restricted via role based security privileges defined within the access control system.	No exceptions noted.
			Inspected the VPN configurations and observed an example login to verify that VPN users were authenticated via username, password, and multifactor authentication.	No exceptions noted.

Description of Control Activities, Tests, Results of Tests, and Criteria Mapping				
Control Number	**Criteria Mapping**	**Control Activity**	**Test of Operating Effectiveness**	**Results**
047	CC6.1; CC6.2	The data center systems are configured to enforce password requirements that include at least one, if not all, of the following requirements: - Minimum password length - Password complexity - Password change requirements	Inspected the data center systems configured password requirements to verify that they include at least one, if not all, of the following requirements: - Minimum password length - Password complexity - Password change requirements	No exceptions noted.
048	CC5.1; CC5.2; CC5.3; CC6.1; CC6.2; CC6.3; CC6.4; CC7.1; CC7.2	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.	Inspected the Corporate Information Security Policy to verify that requirements and procedures were defined regarding system settings, authentication, access, and security monitoring.	No exceptions noted.
049	CC6.2; CC6.4; CC6.5	The physical access to the data center is restricted to the authorized individuals using a card key to unlock the door. Access to the data center is limited to authorized Colohouse employees based on their roles and responsibilities. Access to the data center is approved by data center management. In addition, modification and removal of access is requested by a manager and approved by data center management.	Performed a live walkthrough of all in-scope data centers to verify entrances to the data center are restricted using a card key.	No exceptions noted.
			For a sample of employees hired during the period, inspected ticket documentation to verify access to the data center was approved by data center management.	No exceptions noted.
			For a sample of users terminated during the period, inspected offboarding documentation to verify logical and physical access was removed.	No exceptions noted.

Description of Control Activities, Tests, Results of Tests, and Criteria Mapping				
Control Number	**Criteria Mapping**	**Control Activity**	**Test of Operating Effectiveness**	**Results**
050	CC6.4	Visitors to the facility are required to sign a visitor log upon arrival and must be signed in by an authorized workforce member before a single-day visitor badge that identifies them as an authorized visitor can be issued. Visitor badges are issued for identification purposes only and do not permit access to any secured areas of the facility. All visitors must be escorted by a workforce member when visiting facilities where sensitive system and system components are maintained and operated. Visitors must return their visitor badge at the end of their visit to the security desk.	Performed a live walkthrough of all in-scope data centers to verify visitors and contractors are required to sign in and are escorted by authorized personnel when accessing the facility.	No exceptions noted.
051	CC6.4	Surveillance cameras are located at strategic locations within all data centers to monitor access into the facility and data center floor space as a deterrent to unauthorized access.	Performed a live walkthrough of all in-scope data centers to verify surveillance cameras were located at strategic locations within all data center facilities and data center floor spaces.	No exceptions noted.
052	CC6.4	Policies and procedures are in place to guide personnel in physical security activities.	Inspected the physical security policies and procedures to verify that policies and procedures were in place to guide personnel in physical security activities.	No exceptions noted.
053	CC6.4	A manned reception desk is in place to monitor and control access to the entrance of the office facility during standard business hours.	Performed a live walkthrough of all in-scope data centers to verify a manned reception desk was in place to monitor and control access to the entrance of the office facility during standard business hours.	No exceptions noted.

Description of Control Activities, Tests, Results of Tests, and Criteria Mapping				
Control Number	**Criteria Mapping**	**Control Activity**	**Test of Operating Effectiveness**	**Results**
054	CC6.4	A badge access system controls access to and within the office facility. The sharing of access badges and tailgating are prohibited.	Performed a live walkthrough of in-scope data centers to verify a badge access system controlled access to and within the facility, and verify that badge sharing and tailgating were prohibited.	No exceptions noted.
055	CC6.4; CC6.5; CC6.6	User access to the badge access system is reviewed on an annual basis.	Inspected the badge system user access review for each data center where Colohouse is responsible for physical access to verify user access to the badge system was annually reviewed by management for appropriateness.	No exceptions noted.
056	CC6.6; CC6.7	Network address translation (NAT) functionality is utilized to manage internal IP addresses.	Inspected the NAT configurations for cloud systems to verify that NAT functionality was utilized to manage internal IP addresses.	No exceptions noted.
057	CC6.1; CC6.6	VPN and SSL encryption technologies are used for defined points of connectivity.	Inspected security configurations to verify VPN and SSL, encryption technologies were used for defined points of connectivity.	No exceptions noted.
059	CC6.1; CC6.6; CC6.7	Transmission of digital output beyond the boundary of the system is encrypted.	Inspected the encryption configurations for data in transit and digital certificates to verify that transmission of digital output beyond the boundary of the system was configured to be encrypted.	No exceptions noted.
060	CC5.3; CC8.1	Documented change control policies and procedures are in place to guide personnel in handling system changes to be in accordance with the change management process.	Inspected the Change Enablement Policy and Procedures to verify that documented change control procedures were in place to guide personnel in handling system changes.	No exceptions noted.

Description of Control Activities, Tests, Results of Tests, and Criteria Mapping				
Control Number	**Criteria Mapping**	**Control Activity**	**Test of Operating Effectiveness**	**Results**
061	CC6.6; CC6.7; CC6.8; CC7.2	Antivirus software is installed on workstations and configured to conduct periodic scans to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software. The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available.	Inspected a listing of workstations to verify that antivirus software was installed and active.	No exceptions noted.
			Inspected antivirus software settings to verify the virus protection configurations were in place, and verify the software was configured to push automatic updates.	No exceptions noted.
063	CC4.1; CC4.2; CC6.7; CC6.8; CC7.1; CC7.2	Monitoring software and network hardware (i.e., firewalls) are in place to monitor system security, vulnerabilities, and changes that are made to the system.	Inspected monitoring configurations to verify monitoring software was in place to monitor system security, vulnerabilities, and changes made to the system.	No exceptions noted.
			Inspected monitoring systems to verify firewall rule configurations and server protection configurations were in place to monitor system security, vulnerabilities, and changes made to the system.	No exceptions noted.
064	CC7.2; A1.1; A1.2	Environmental systems are monitored and issues related to environmental equipment are documented and resolved timely by network operations center ("NOC") personnel.	Inspected monitoring configurations to verify environmental systems were monitored for issues related to environmental equipment.	No exceptions noted.
			For a sample of reported environmental issues, inspected ticket documentation to verify issues related to environmental equipment were documented and resolved timely by network operations center ("NOC") personnel.	No exceptions noted.

Description of Control Activities, Tests, Results of Tests, and Criteria Mapping				
Control Number	**Criteria Mapping**	**Control Activity**	**Test of Operating Effectiveness**	**Results**
066	CC2.3; CC4.2; CC5.3; CC6.7; CC6.8; CC7.2; CC7.3; CC7.4; CC7.5	Documented incident response policies and procedures are in place to guide personnel in the event of an incident.	Inspected the Incident Management Policy to verify that documented incident response policies and procedures were in place to guide personnel in the event of an incident.	No exceptions noted.
067	CC8.1	All changes to the Colohouse systems must be logged and implemented as per the documented change management policies. All changes, are initiated by a request, authorized for implementation, tested (if needed) and approved by clients and Colohouse management prior to commencing any work in the data center.	Inspected change documentation and inquired with the SVP Technical Operations to verify that no infrastructure changes occurred during the examination period.	No occurrences to test.
068	CC8.1	Access to the data center for the purposes of implementing changes is limited to authorized Colohouse employees, clients, and vendors who are authorized to access the data center floor space.	Inspected client access listing configurations and employee access review documentation to verify access to the data center for the purposes of implementing changes was restricted to authorized employees, clients, and vendors.	No exceptions noted.
070	CC8.1	System change requests are documented and tracked in a ticketing system, changes are approved by management and tested prior to implementation. Types of testing performed depend on the nature of the change.	Inspected change documentation and inquired with the SVP Technical Operations to verify that no system change requests occurred during the examination period.	No occurrences to test.
072	CC8.1	Documented change control policies and procedures are in place to guide personnel in implementing changes in an emergency situation.	Inspected the Change Enablement Policy and Procedures to verify procedures were defined that guide personnel in implementing changes in an emergency situation.	No exceptions noted.

Description of Control Activities, Tests, Results of Tests, and Criteria Mapping				
Control Number	**Criteria Mapping**	**Control Activity**	**Test of Operating Effectiveness**	**Results**
073	CC2.1; CC3.1; CC3.2; CC3.3; CC3.4; CC4.1; CC4.2; CC5.1; CC5.2; CC9.1	Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances.	Inspected the annual risk assessment to verify a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances was defined.	No exceptions noted.
074	CC2.1; CC3.1; CC3.2; CC3.3; CC3.4; CC4.1; CC4.2; CC5.1; CC5.2; CC9.1	A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	Inspected risk assessment documentation to verify management performed an annual risk assessment and identified internal and external threats and vulnerabilities that could impair system commitments and requirements.	No exceptions noted.
075	CC9.2	Colohouse has developed a data center management policy and plan that assesses and manages risks associated with vendors and business partners.	Inspected the Vendor Management Policy to verify procedures for assessing and managing risks associated with vendors and business partners were defined.	No exceptions noted.
			Inspected the vendor risk assessment to verify risks associated with vendors and business partners were assessed by management.	No exceptions noted.
076	CC2.1; CC9.2	Management has defined a third-party vendor risk management process that specifies the process for evaluating third-party risks based on identified threats and the specified tolerances.	Inspected the Vendor Management Policy to verify that management had a defined a third-party vendor risk management process that specified the process for evaluating third-party risks based on identified threats and the specified tolerances.	No exceptions noted.

Description of Control Activities, Tests, Results of Tests, and Criteria Mapping				
Control Number	**Criteria Mapping**	**Control Activity**	**Test of Operating Effectiveness**	**Results**
077	CC9.1; A1.3	Disaster recovery and backup restoration testing is performed on an annual basis, test results are reviewed and contingency plans are adjusted as needed.	Inspected the results of the annual business continuity and disaster recovery testing to verify annual testing of the business continuity and disaster recovery plan was performed, and verify test results were reviewed and contingency plans were adjusted as needed.	No exceptions noted.
			Inspected the results of the annual backup restoration testing performed for Colohouse Cloud to verify that annual restoration testing was performed.	No exceptions noted.

Trust Services Criteria with Supporting Control Mapping

The table below defines the applicable trust services criteria and maps controls supporting the criteria.

Trust Services Criteria with Supporting Control Mapping		
TSC Reference	**Criteria**	**Supporting Control Activity**
CC1.0 Control Environment		
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	013; 014; 019; 022; 025; 028; 037
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	001; 015; 017; 020
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	012; 017; 018; 019; 021; 042
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	012; 013; 014; 018; 019; 022
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	012; 013; 014; 017; 018; 019
CC2.0 Communication and Information		
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	021; 025; 028; 035; 036; 037; 073; 074; 076
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	012; 013; 014; 018; 019; 025; 028; 029; 033; 042
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	031; 032; 033; 034; 066
CC3.0 Risk Assessment		
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	035; 036; 073; 074
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	021; 035; 036; 073; 074
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	036; 073; 074
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	021; 036; 073; 074
CC4.0 Monitoring Activities		
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	001; 003; 021; 027; 036; 039; 042; 063; 073; 074

Trust Services Criteria with Supporting Control Mapping		
TSC Reference	**Criteria**	**Supporting Control Activity**
CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	001; 003; 027; 036; 038; 042; 063; 066; 073; 074
CC5.0 Control Activities		
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	025; 028; 035; 036; 037; 042; 048; 073; 074
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	025; 028; 035; 037; 042; 048; 073; 074
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	019; 025; 028; 033; 037; 042; 048; 060; 066
CC6.0 Logical and Physical Access Controls		
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	045; 046; 047; 048; 057; 059
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	045; 046; 047; 048; 049
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	045; 046; 048
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	044; 048; 049; 050; 051; 052; 053; 054; 055
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	045; 049; 055
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	027; 038; 046; 055; 056; 057; 059; 061
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	027; 038; 039; 045; 056; 059; 061; 063; 066
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	027; 038; 039; 045; 061; 063; 066

Trust Services Criteria with Supporting Control Mapping		
TSC Reference	**Criteria**	**Supporting Control Activity**
CC7.0 System Operations		
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	027; 033; 039; 048; 063
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	027; 033; 048; 061; 063; 064; 066
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	001; 038; 066
CC7.4	The entity responds to identified security incidents by executing a defined incident-response program to understand, contain, remediate, and communicate security incidents, as appropriate.	001; 033; 038; 066
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	005; 038; 066
CC8.0 Change Management		
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	060; 067; 068; 070; 072
CC9.0 Risk Mitigation		
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	005; 036; 073; 074; 077
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	021; 075; 076
A1.0 Additional Criteria for Availability		
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	001; 002; 003; 004; 064
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	002; 003; 004; 005; 006; 007; 008; 021; 064
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	002; 005; 077

weaver

Assurance • Tax • Advisory

For more information regarding Weaver, visit
our IT Advisory Services page: