COLOHOUSE LLC

System and Organization Controls (SOC 2) Type 2 Report

Report on Colohouse LLC's
Description of Its System and on the Suitability of the
Design and Operating Effectiveness of Its Controls
Relevant to Security, Availability, and Confidentiality
Throughout the Period
September 1, 2022 to August 31, 2023

BUCHBINDER

COLOHOUSE LLC

System and Organization Controls (SOC 2) Type 2 Report

Report on Colohouse LLC's
Description of Its System and on the Suitability of the
Design and Operating Effectiveness of Its Controls
Relevant to Security, Availability, and Confidentiality
Throughout the Period
September 1, 2022 to August 31, 2023

Table of Contents

COLOHOUSE LLC

System and Organization Controls (SOC 2) Type 2 Report

Report on Colohouse LLC's
Description of Its
System and on the Suitability of the
Design and Operating Effectiveness of Its Controls
Relevant to Security, Availability, and Confidentiality
Throughout the Period
September 1, 2022 to August 31, 2023

Table of Contents

BUCHBINDER

Section I – Independent Service Auditor's Report

To the Management of Colohouse LLC

Scope

We have examined Colohouse LLC's ("Colohouse") description of Colohouse's system entitled "Colohouse LLC's Description of the System" throughout the period September 1, 2022 to August 31, 2023 ("description") based on the criteria for a description of a service organization's system set forth in DC 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, 2022 to August 31, 2023, to provide reasonable assurance that Colohouse's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality ("applicable trust services criteria") set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)* in AICPA, *Trust Services Criteria*.

The description indicates that certain 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.

Colohouse uses subservice organizations 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 organizations' 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 organizations' 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. In Section I, Colohouse has provided the accompanying assertion titled "Colohouse LLC's Management's Assertion" ("assertion") about the description and the suitability of design and operating effectiveness of controls stated therein. Colohouse is also 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 AICPA. 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 a 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 examination 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 report users may consider important to meet their informational needs. There are inherent limitations in 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 or 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 we tested and the nature, timing, and results of those tests are listed in Section III, "Applicable Trust Services Criteria for Security, Availability, and Confidentiality, Related Controls and Information Provided by the Independent Service Auditor" of this report.

Opinion

In our opinion, in all material respects:

(a) The description presents Colohouse's system that was designed and implemented throughout the period September 1, 2022 to August 31, 2023 in accordance with the description criteria.

(b) The controls stated in the description were suitably designed throughout the period September 1, 2022 to August 31, 2023 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.

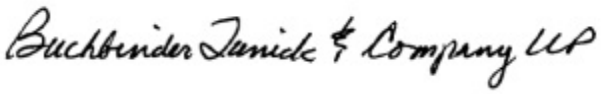
(c) The controls stated in the description operated effectively throughout the period September 1, 2022 to August 31, 2023 to provide reasonable assurance that Colohouse's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organizations' controls and complementary user entity controls assumed in the design of Colohouse's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section III, is intended solely for the information and use of Colohouse, user entities of Colohouse's system during some or all of the period September 1, 2022 to August 31, 2023, business partners of Colohouse subject to risks arising from interactions with the 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 user entity controls and complementary subservice organizations 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 the specified parties.



BUCHBINDER TUNICK & COMPANY LLP

Little Falls, NJ
October 27, 2023

36 NE 2nd Street, Suite 400, Miami,
866-790-2656
hello@colohouse.com
www.colohouse.com

Colohouse LLC's Management's Assertion

We have prepared the accompanying description of Colohouse's colocation and managed services system titled "Colohouse LLC's Description of the System" throughout the period September 1, 2022 to August 31, 2023 ("description") based on the criteria for a description of a service organization's system set forth in DC 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 the colocation and managed 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 their service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality ("applicable trust services criteria") set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)* in AICPA*, Trust Services Criteria*.

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 the service organization's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of the service organization's controls.

Colohouse uses subservice organizations to provide data center services. The description indicates that complementary subservice organizations' 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 organizations' controls assumed in the design of Colohouse's controls. The description does not disclose the actual controls at the subservice organizations.

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

(a) The description presents Colohouse's colocation and managed services system that was designed and implemented throughout the period September 1, 2022 to August 31, 2023 in accordance with the description criteria.

(b) The controls stated in the description were suitably designed throughout the period September 1, 2022 to August 31, 2023 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, 2022 to August 31, 2023 to provide reasonable assurance that Colohouse's service commitments and system requirements were achieved based on the applicable

36 NE 2nd Street, Suite 400, Miami,
866-790-2656
hello@colohouse.com
www.colohouse.com

trust services criteria, if complementary subservice organizations' controls and complementary user entity controls assumed in the design of Colohouse's controls operated effectively throughout that period.

Very truly yours,

Ross Woodham

Ross Woodham
Chief Legal Officer, Colohouse

Section II – Colohouse LLC's Description of the System

Services Provided

Colohouse

Colohouse is a retail colocation, hosting, and cloud services provider, and may be referred to elsewhere as "data center services". Colohouse provides a digital foundation that connects our customers with impactful technology solutions and services. Our managed data center and cloud infrastructure paired with key edge locations and reliable connectivity allow our customers to confidently scale their application and data while optimizing for cost, performance, and security.

Colohouse's headquarters are designated at 36 NE 2nd Street, Suite 400 Miami, FL 33132 and is also the site of a primary data center location in Miami. There are also other corporate and data center supporting functions in designated office locations in Texas, Utah, Colorado, Illinois and New York.

Colohouse predominately maintains and supports its data center sites through the leasing of purpose-built data center space and critical infrastructure operated by the defined **Subservice Organizations** and specified by the **System Boundaries** sections below. Colohouse owns and operates one (1) data center facility located in Latham, NY.

Description of Services Provided

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)

Principal 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, availability, and confidentiality 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, availability, and confidentiality 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, availability, confidentiality; 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.

Components of the System Used to Provide the Services

Colohouse's system is comprised of the following components:

- **System Boundaries -** the listing of the data centers in scope for this report.
- **Infrastructure -** the hardware components of a system (e.g., facilities, equipment, networks).
- **Software -** the programs and operating software of a system (e.g., systems, applications, and utilities).
- **People -** the personnel involved in the operation and use of a system (e.g., operators, users, and managers).
- **Data -** the information used and supported by the system (e.g., files, databases, and tables).
- **Process and Procedures -** the automated and manual procedures involved in the operation of a system (e.g., preventative and detective control activities).

System Boundaries

A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, data, and processes and procedures.

The scope of the review includes the services performed at the data center facilities located in the metropolitan areas listed below.

Specifically, the following data center sites were included within the scope of this report:

- 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)
- San Jose, CA – 5 Great Oaks Boulevard (Equinix SV11)
- Ashburn, VA – 22175 Beaumeade Circle (Equinix DC21)

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.

Primary Infrastructure	
Hardware	**Purpose**
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

Primary software used to provide Colohouse services includes the following:

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.

Primary Software		
Software	**Operating System**	**Purpose**
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 processes are organized to help ensure business processes are executed in an efficient and effective manner and that an adequate segregation of duties is maintained within the firm. All jobs have been defined within this organizational structure to help ensure that adequate segregation of duties is maintained while assigning individual job responsibilities. Individual job responsibilities are communicated to employees, supervisors, and managers through formal job descriptions.

The following organizational elements have been established to support an adequate segregation of functions:

- **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 ("HR") -** 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.

- **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.

Data

Data is managed in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer contracts. Data is captured which is utilized by Colohouse in delivering their services. Such data includes, but is not limited to, the following:

- Alert notifications and monitoring reports generated from the monitoring applications

- Alert notifications received from automated physical and environmental monitoring systems

- Incident reports documented via the ticketing systems

- Client configurations and billing information

- Client interface files and inputs

- Output reports

- Security access records

- Video surveillance information

Processes and Procedures

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to the Colohouse policies and procedures that define how services should be delivered. These are located on the Colohouse intranet and can be accessed by any team member.

Physical Security and Environmental Controls

Access to Colohouse data centers is controlled by building security, facility coordinators and other Colohouse employees in addition to the badge access systems, to prevent unauthorized users from entering the facility. In addition, a combination of security guards and/or other Colohouse employees are utilized at Colohouse facilities to restrict access. The data center and other sensitive areas are physically segregated from general building access and require special access privileges. Data center access is monitored 24 hours a day, 7 days per week, through video surveillance and on-site security guards to prevent unauthorized access.

Customers without badge/biometric access must contact the appropriate Colohouse staff to access the facility and must be on the authorized user listing. New hires that require badge access must be approved by senior management before access is granted. Terminated employee access is removed immediately. Visitors, including contractors, to the Colohouse facilities are required to sign-in with building security located in the lobby and must be escorted by an appropriate Colohouse employee. Visitors will also be required to sign in before entering the facility.

Customer access lists are configured based on the access control list submitted during the customer onboarding process. Customer access is configured to expire on a periodic basis and requires revalidation by the customer single point of contact (“SPOC”). Only authorized users may request changes to the data center user access listings. Any updates to a customer's access listing are communicated to building security and/or other administrators responsible for restricting access to Colohouse facilities.

On a quarterly basis, a physical access review of data center access is performed for Colohouse employees, vendors and customers.

Surveillance cameras are located at strategic locations within the data centers as a deterrent to unauthorized access. Surveillance recordings are maintained for a minimum of 30 days on DVR.

Access to cages is secured by a key, badge or biometric access system to prevent unauthorized access. In addition, access to the server racks is secured by a custom key code determined by the client. In case of an emergency, Colohouse's management maintains a master key to access the server cages and racks.

Uninterruptible power supply (“UPS”) units are located inside each of the facilities. Municipal electricity powers the building, which powers the UPS system. The primary UPS is monitored daily, and performance results are monitored. All Colohouse facilities are equipped with backup generators that automatically supply power to Colohouse facilities in the event of a commercial power failure. Environmental equipment, including HVAC, UPS, PDUs, generators, adequate lighting and fire suppression are also present at each facility. Fire, smoke and water detectors are installed throughout the facilities. Air conditioning units in Colohouse facilities are maintained separate from and independent of the building's general air conditioning systems and maintain

temperature and humidity conditions appropriate for hardware. In addition, power, temperature, humidity and functioning of critical environmental equipment are monitored in each facility. Any issues discovered in environmental systems are documented and resolved in a timely manner.

Colohouse data centers have a redundant configuration and multiple power panels with circuit breakers to minimize the disruption of operations during a power outage. Automatic transfer switches ("ATS") are in place to utilize the generators and uninterruptible power supply ("UPS") in the case of an emergency. In addition, at least annually, the UPS and generators are tested with the critical load through the use of ATS. To help ensure operations during prolonged power outages, generators undergo scheduled maintenance on a quarterly basis. Maintenance contracts are in place for all significant electrical equipment (generators, power panels and heating, ventilating, and air conditioning ("HVAC") systems).

Raised and non-raised floors are in place throughout Colohouse's data center server rooms to protect servers from flood damage. On an annual basis, the leak detection systems in Colohouse's data centers are tested to prevent water damage to the servers located in the data centers.

System Monitoring

Colohouse maintains documented problem resolution policies and procedures for its data center environment to ensure problems and incidents are documented, tracked and resolved in a timely manner. An service incident event is classified as an unexpected interruption of service, and includes, but is not limited to, network hardware failure, user error, network security breach and software failure. Problems may be identified internally by Colohouse or externally by customers and are classified as incidents. In addition, security, availability, and confidentiality incidents and complaint procedures are outlined in the Operating Principles and Procedures.

Network Operations Center ("NOC") and security events are recorded in the ticketing and email system and reported to management.

Customer service requests are logged, reviewed, and appropriate and timely action is taken for each request. Any changes that may affect customers are appropriately communicated through e-mail. In addition, 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. Management conducts weekly executive meetings to discuss operational metrics and logs.

Logical Access

Colohouse uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. Resources are protected through the use of native system security and add-on software products that identify and authenticate users and validate access requests against the users' authorized roles in access control lists. In the event incompatible responsibilities cannot be segregated, Colohouse implements monitoring of one or more of the responsibilities. Monitoring must be performed by a superior without responsibility for performing the conflicting activities or by personnel from a separate department.

Employees sign on to the Colohouse corporate systems using service directory managed credentials for access to workstations or laptops. Passwords must conform to defined password standards and are enforced through parameter settings in Active Directory, or equivalent directory services. According to NIST established standards passwords are implemented as passphrases and are not changed unless there is a requirement (e.g., an employee is terminated or forgets their password, or a suspected account compromise).

Employees accessing the system from outside the Colohouse network are required to use VPN with either user account credentials in combination with a certificate or token-based two-factor authentication system. Employees are issued tokens, soft token and/or certificates upon VPN configuration access. Vendor personnel are not permitted to access the system from outside the Colohouse network.

Customer employees access available customer portal services over the Internet using the SSL functionality of their web-browser and or through VPN access to their hosted services. These customer employees must supply a valid user ID and password to gain access to customer cloud resources. Passwords must conform to password configuration requirements configured on the virtual devices using the virtual server administration account.

Upon employee termination, access is revoked by disabling accounts. The access list is audited at least annually to ensure all terminated employees have been properly deactivated.

Computer Operations – Backups

Customer data is backed up and monitored by operations personnel for completion and exceptions. In the event of an exception, operations personnel perform troubleshooting to identify the root cause and then re- run the backup job immediately or as part of the next scheduled backup job depending on customer indicated preference within the documented work instructions.

The backup storage area network is physically secured in locked cabinets and/or caged environments within their data centers. The backup infrastructure resides on private networks logically secured from other networks.

Contracted customer off-site backups are self-managed and Colohouse's operations personnel only guarantee the availability and security of the platform, not the schedules and/or rotations. The ability to recall backup media from the off-site storage facility is restricted to authorized operations personnel and customer employees with access to their isolated storage volumes.

Computer Operations – Availability

Incident response policies and procedures are in place at Colohouse to guide personnel in reporting and responding to information technology incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents. Incident response procedures are in place to identify and respond to incidents on the network.

Colohouse monitors the capacity utilization of physical and computing infrastructure both internally and for customers to ensure that service delivery matches service level agreements. Colohouse evaluates the need for additional infrastructure capacity in response to growth of existing customers and/or the addition of new customers. Infrastructure capacity monitoring includes, but is not limited to, the following infrastructure:

- Data center space, power and cooling
- Disk storage
- Computing power
- Server stock
- Network bandwidth

Change Control

Colohouse maintains documented Systems Development Life Cycle ("SDLC") policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, and required approval procedures.

Colohouse does not do development as a component of the data center services. Change control procedures for system components not the responsibility of Colohouse are the responsibility of the customers.

Colohouse has implemented a patch management process to ensure contracted managed hosting customer and infrastructure systems are patched in accordance with vendor recommended operating system patches. Colohouse's operations personnel reviews patches to determine whether the patches are applied. In certain cases, operations personnel may coordinate with customers to identify the best way forward.

Customers and Colohouse personnel are responsible for determining the risk of applying or not applying patches based upon the security, availability, and confidentiality impact of those systems and any critical applications hosted on them. Colohouse staff validate that all patches have been installed and, if applicable, that reboots have been completed.

Data Communications

Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Network address translation ("NAT") functionality is utilized to manage internal IP addresses. Administrative access to the firewall is restricted to authorized employees.

Redundancy is built into the system infrastructure supporting the data center services to help ensure that there is no single point of failure that includes firewalls, routers, and servers. In the event that a primary system fails, the redundant hardware is configured to take its place.

Vulnerability scanning is performed by Colohouse IT/Security staff against internet accessible systems after being notified of changes . Internal vulnerability scanning is performed throughout the year. Colohouse uses industry standard scanning technologies and a formal methodology specified by Colohouse. These technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on an as needed basis and as authorized.

Authorized employees may access the system from the Internet through the use of leading VPN technology. Employees are authenticated through the use of a token-based two-factor authentication system.

Disaster Recovery

Disaster Recovery ("DRP") Plans and operating procedures are in place to guide personnel in the decisions, responsibilities and requirements following disruptions to normal operations. A disaster incident can result from a number of accidental, malicious or environmental events such as fire, flood, terrorist attack, human error, and software or hardware failures.

Relevant Aspects of the Control Environment, Risk Assessment Process, Information and Communication Systems, and Monitoring Controls

Control Environment

Colohouse maintains a control environment to ensure the security, availability, and confidentiality of Colohouse's data and systems. Colohouse has developed and implemented numerous policies to guide the operations of the company. Colohouse's control environment reflects the philosophy of senior management concerning the importance of the security, availability, and confidentiality of company data and systems. The importance of security, availability, and confidentiality is emphasized through the establishment and communication of policies and procedures and is supported by investment in resources and people to carry out the policies. In designing its controls, Colohouse has taken into consideration the relevance of controls to meet the specific trust criteria.

The following is a description of the key components of internal control:

Management's Control Philosophy

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.

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.

Commitment to Competence

Colohouse's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into the requisite skills and knowledge.

Organizational Structure

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.

Authority and Responsibility

Specific authority and responsibilities are clearly established throughout Colohouse and are communicated by its senior management team, including (1) management philosophy and operating style, (2) organizational structure, (3) employee job descriptions, and (4) policy and procedure manuals.

Human Resources Policies and Practices

Suitable qualifications/eligibility for employment are required which are verified by the human resources department, and management maintains written policies and procedures for hiring employees and independent contractors. Hiring policies require a minimum level of education and experience, completion of all application forms, references, background and criminal record checks, as well as execution of confidentiality statements. Human resources maintains formal job descriptions that have been established for key positions and are expanded to address needs as new responsibilities are identified. Job responsibilities correspond with organizational departments. Organizational charts are defined and reviewed and updated regularly.

Specific control activities that the service organization has implemented in this area are described below:

- New employees are required to sign acknowledgement forms for the employee handbook, which includes confidentiality obligations following new hire orientation on their first day of employment.

- Colohouse new hires undergo criminal background checks. The results of the background checks are reviewed by management and/or recruiters to determine final employment eligibility.

- Evaluations for each employee are performed on an annual basis.

- Employee termination procedures are in place to guide the termination process and are documented in a termination form.

- Employee training is accomplished through supervised on-the-job training, in-house courses, and external educational programs. Certain positions may require completion of specific training or licensing.

- A security awareness program has also been implemented to mitigate risk and communicate security best practices to Colohouse employees.

Risk Assessment Process

Colohouse’s risk assessment process identifies and manages risks that could potentially affect Colohouse. Colohouse's risk assessment process generally consists of the following elements:

- Assessing the sufficiency of corporate policies, procedures, systems and other arrangements in place to control risk.
- Identifying potential risks in Colohouse's technology, products, security and services.
- Determining the level of severity for identified risk factors when evaluating the potential impact of the identified risk factors on the operating effectiveness of existing controls.
- Identifying potential sources of risk and recommending areas for management to develop and implement policies and procedures to mitigate the identified risk areas.
- Monitoring and evaluating the operating effectiveness of existing controls in light of changes resulting from growth, new or renovated information systems, regulatory changes, new personnel and external security risk factors.
- Monitoring the regulatory environment to identify proposed and/or new regulations and determine the effect such regulations may have on Colohouse's service offerings.

Management has implemented various measures to manage risks identified by the risk assessment process. Specific risks that have been identified by management as significant to Colohouse include the following:

- **Operational Risk -** changes in the environment, staff, or management personnel or client work orders are not processed on a timely basis

- **Strategic Risk -** new technologies, changing business models, and shifts within the industry

- **Compliance Risk -** legal and regulatory changes

- **Reputational Risk –** data center facilities are not adequately secured or provide the necessary environmental and recoverability controls.

- **Technological Risk –** system failures or the disclosure of client data to an unauthorized or an outside source.

Information and Communication Systems

Information and communication are integral components of Colohouse's internal control system. Colohouse controls depend upon Colohouse identifying, capturing, and exchanging information in the form and timeframe necessary to conduct, manage, and control the entity's operations. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, information technology. At Colohouse, information is identified, captured, processed, and reported by various information systems as well as through conversations with clients, vendors, regulators, and employees.

Various recurring calls are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization. General updates to entity-wide security policies and procedures are usually communicated to the appropriate Colohouse personnel via company meetings, e-mail messages and/or the SharePoint portal.

Colohouse has information technology policies to help ensure that employees understand their individual roles and responsibilities concerning security, availability, and confidentiality, and to ensure that any significant issues are communicated in a timely manner to management. In addition, Colohouse offers training programs for its employees so that they can be better informed on how to perform their job functions. The quality of system-generated information affects management's ability to make appropriate decisions in controlling the entity's activities (see the **Components of the System Used to Provide the Services** section for more details on the information systems).

Monitoring Controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Colohouse's management performs monitoring activities to continuously assess the quality of internal controls over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures are also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-Going Monitoring

Colohouse's management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management's close involvement in Colohouse's operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of Colohouse's personnel.

Reporting Deficiencies

An internal tracking tool is utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions. In addition, management obtains and reviews relevant system and organization control ("SOC") reports for relevant service providers and performs assessments of the service providers performance and control environment as part of their vendor management processes.

Subservice Organizations

Colohouse uses the below listed subservice organizations to outsource certain functions or supplement their services. The services provided are described below:

- Digital Realty Data Center Solutions
- fifteenfortyseven Critical Systems Realty
- Iron Mountain
- Equinix
- CyrusOne

The subservice organizations provide physical security and environmental data center services that support the entity's infrastructure. The complimentary subservice organizations control considerations for these subservice organizations include the following which are linked to the indicated security trust services criteria:

Subservice Organization		
Category	Criteria	Control
Security	CC6.4	Physical access controls are in place to restrict access to and within the data center facilities.
		Physical access requests are documented and require the approval of the site manager.
		A review of employees and contractors with physical access to customer suites is performed on a quarterly basis and unnecessary access is identified, modified, and removed as necessary.
		A termination notification ticket is completed by HR and physical access is revoked by the corporate security team for employee and contractor terminations within one business day of termination.
		Visitors are required to surrender their badges upon exit. Access badges for visitors that do not require an escort are configured to expire at the end of the day.
		Surveillance cameras are in place to monitor and record access to and within the data centers. Surveillance cameras are located along the building perimeters and within the data centers.
		Digital surveillance systems are required to retain video footage for the data centers for a minimum of 30 days.
Availability	A1.2	Facilities are equipped with a fire suppression system.
		Facilities are equipped with a fire detection system that is regularly maintained.
		Critical servers are equipped with battery backup systems.
		Critical servers are properly cooled.

Services provided by Colohouse to user entities and the related controls should be considered in conjunction with the complementary subservice organizations controls. It is not feasible for the controls related to the colocation and managed services system to be achieved solely by Colohouse. Therefore, each user entity's internal control environment must be evaluated in conjunction with Colohouse's controls described in Section III of this report taking into account the related complementary subservice organizations controls expected to be implemented at the subservice organizations as described above.

Colohouse management, along with the subservice organizations, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, Colohouse performs monitoring of the subservice organizations controls, including performing the following procedures:

- Reviewing and reconciling output reports
- Holding periodic discussions with vendors and subservice organizations
- Making regular site visits to vendor and subservice organization's facilities
- Reviewing attestation reports over services provided by vendors and the subservice organizations

Changes to the System and Major Incidents During the Period

There were no changes that are likely to affect report users' understanding of how the system is used to provide the services during the period from September 1, 2022 to August 31, 2023. In addition, there were no system incidents that were identified as of this date that resulted in a significant impairment of Colohouse's ability to achieve its service commitments and system requirements.

Complementary User Entity Controls

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

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the trust services criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

- User entities are responsible for understanding and complying with their contractual obligations to Colohouse (CC2.3 and CC3.4).

- User entities are responsible for notifying Colohouse of changes made to technical or administrative contact information (CC2.3).

- User entities are responsible for maintaining their own system(s) of record (CC8.1).

- User entities are responsible for ensuring the supervision, management, and control of the use of Colohouse services by their personnel (CC6.1).

- User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Colohouse services (A1.2 and A1.3).

- User entities are responsible for providing Colohouse with a current or updated list of

approvers for security and system configuration changes.

- User entities are responsible for immediately notifying Colohouse of any actual or suspected information security breaches or incidents, including compromised user accounts, including those used for integrations and secure file transfer (CC7.3, CC7.4, CC7.5).

- User entities must actively manage the physical security of their suites and cabinets and the respective access lists. These include granting access, removing access and reviewing access to their suites and cabinets on a periodic basis (CC6.2, CC6.3, CC6.4).

- User entities are responsible to ensure requests submitted to Colohouse are complete, accurate and timely, and follow Colohouse processes (CC8.1).

- User entities are responsible for configuring, maintaining, and assessing best practice security controls for their servers, systems and applications running in or on Colohouse colocation, hosting, and cloud service, including physical or virtual server operating systems, appliances, databases, and applications.

- User entities are responsible for the secure destruction of their data and software.

- User entities are responsible for the integrity of data and the backup of data stored in Colohouse facilities.

- User entities are responsible for the maintenance records of destruction of hardware.

- User entities are responsible for the management of logical access of their data.

- User entities are responsible for their system backup and recovery services.

- User entities must actively manage their IT systems that are housed in Colohouse facilities (CC6.1, A1.1).

- User entities are responsible for the initiation, communication and approval of change requests or modifications to appropriate Colohouse personnel using pre-established communication means (CC8.1).

- User entities are responsible for the appropriate follow-up procedures to monitor reported problems or special processing requests (CC7.3, CC7.4, CC7.5).

The complementary user-entity control considerations presented above do not represent a comprehensive listing of the controls that should be employed within each user entity. Other controls may be required at user entities.

Applicable Trust Services Criteria and the Related Controls

Although the applicable trust services criteria, related controls, and management responses to deviations, if any, are presented in Section III - Applicable Trust Services Criteria for Security, Availability, and Confidentiality, Related Controls and Information Provided by the Independent Service Auditor, they are an integral part of Colohouse's description of its system throughout the period September 1, 2022 to August 31, 2023. They are presented in Section III to eliminate the redundancy that would result from listing them in this section and repeating them in Section III.

All the trust services criteria and controls presented in Section III relating to security, availability, and confidentiality are relevant for the purposes of this report.

Section III – Applicable Trust Services Criteria for Security, Availability, and Confidentiality, Related Controls and Information Provided by the Independent Service Auditor

The purpose of this report is to provide management of Colohouse, user entities, and other specified parties with information about controls at Colohouse that are intended to mitigate risks related to the security, availability, and confidentiality criteria set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.*

This section presents the following information provided by Colohouse:

- Detailed listings of the security, availability, and confidentiality criteria.
- The control activities established and specified by Colohouse to achieve the controls as stipulated by the trust services criteria.

Also included in this section is the following information provided by Buchbinder Tunick & Company LLP:

- A description of the testing performed by the service auditor to determine Colohouse's controls were operating with sufficient effectiveness to achieve specified control activities.
- The service auditor determined the nature, timing, and extent of the testing performed.
- The results of the service auditor's tests of operating effectiveness.

We also performed procedures to evaluate whether the information provided by the service organization 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. Information we utilized as evidence may have included, but was not limited to:

- Standard "out-of-the-box" reports as configured within the system.
- Parameter-driven reports generated by Colohouse's systems.
- Custom-developed reports that are not standard to the application such as scripts, report writers, and queries.
- Spreadsheets that include relevant information utilized for the performance or testing of a control.
- Prepared analyses, schedules, or other evidence manually prepared and utilized by Colohouse to perform certain control activities.

Our procedures to evaluate whether this information was sufficiently reliable included (a) obtaining evidence regarding the accuracy and completeness of source data, and (b) the creation and modification of applicable report logic and parameters. While these procedures were not specifically listed in this section, they were completed as a component of our evaluation of whether the information is sufficiently precise and detailed to fully support the controls identified by Colohouse.

Common Criteria for the Security, Availability, and Confidentiality Trust Services Criteria

CC1.0 - Common Criteria Related to the Control Environment

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	Colohouse follows best practice hiring and training procedures to ensure that the personnel responsible have requisite qualifications and skills to fulfill their responsibilities. Written job descriptions exist for all key firm personnel and background checks are performed on all new employees. An employee handbook and code of conduct are documented to communicate workforce conduct standards and enforcement procedures.	Inspected the hiring procedures to verify that hiring and training procedures are in place to ensure that the personnel responsible have requisite qualifications and skills to fulfill their responsibilities. Inspected written job descriptions for key management and IT personnel to determine whether the job descriptions include responsibilities Inspected the employee handbook to determine that an employee handbook and code of conduct were documented to communicate workforce conduct standards and enforcement procedures.	No Exceptions Noted.

CC1.0 - Common Criteria Related to the Control Environment (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	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. Sanction policies, which include probation, suspension and termination, are in place for employee misconduct.	For a sample of new employees, inspected the results of background checks to determine whether a background check was performed. For a sample of new employees, obtained signed code of conduct and statement of confidentiality documents and verified that new personnel are required to read and accept the code of conduct, the employee handbook, and the statement of confidentiality at the time of hire. Inspected the employee handbook to determine that sanction policies, which include probation, suspension and termination, were in place for employee misconduct.	No Exceptions Noted.

CC1.0 - Common Criteria Related to the Control Environment (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Colohouse's CEO exercises oversight of the development and performance of internal control and company performance and objectives.	Through inquiry with the CEO confirmed that the CEO exercises oversight of the development and performance of internal control and company performance and objectives as part of the CEO's monitoring and control of the firm.	No Exceptions Noted.
		Senior management meetings are held with key management personnel to discuss the firm's performance and provide oversight of Colohouse's internal control environment.	Obtained documentation relating to senior management meetings and verified that the meetings are held with key management personnel, are documented, and that these meetings discuss the firm's performance and provide oversight of Colohouse's internal control environment.	
		Executive management roles and responsibilities are documented and reviewed annually.	Inspected executive management job descriptions with revision history to determine that executive management roles and responsibilities were documented and reviewed annually.	

CC1.0 - Common Criteria Related to the Control Environment (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	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.	Obtained the most recent organizational chart and verified through inquiry and observation that Colohouse has developed an organizational structure and reporting lines.	No Exceptions Noted.
		Roles and responsibilities are defined in written job descriptions and communicated to managers and their supervisors.	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.	
		Colohouse provides annual security training for employees and the results are monitored by management in order to track compliance with training requirements.	Obtained training documentation and verified that annual security training is provided for employees and that the results are monitored by management in order to track compliance with training requirements.	

CC1.0 - Common Criteria Related to the Control Environment (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Operational and security policies are reviewed and updated, if necessary, on an annual basis. Executive management has established proper segregations of duties for key job functions and roles within the organization. A vendor risk assessment is performed on an annual basis which includes reviewing the activities performed by third parties.	Obtained documentation and verified that the policies are reviewed and updated, if necessary, on an annual basis. Inspected the organizational chart and a sample of job descriptions to determine that executive management established proper segregations of duties for key job functions and roles within the organization. Inspected the vendor risk assessment policies and procedures and the completed vendor risk assessment to determine that a vendor risk assessment was performed on an annual basis which included reviewing the activities performed by third parties.	No Exceptions Noted.

CC1.0 - Common Criteria Related to the Control Environment (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Colohouse follows best practice hiring and training procedures to ensure that the personnel responsible have requisite qualifications and skills to fulfill their responsibilities. Written job descriptions exist for all key firm personnel and background checks are performed on all new employees. Colohouse provides annual security training for employees and the results are monitored by management in order to track compliance with training requirements.	Inspected the hiring procedures to verify that hiring and training procedures are in place to ensure that the personnel responsible have requisite qualifications and skills to fulfill their responsibilities. Inspected written job descriptions for key management and IT personnel to determine whether the job descriptions include responsibilities For a sample of new employees, inspected the results of background checks to determine whether a background check was performed. Obtained training documentation and verified that annual security training is provided for employees and that the results are monitored by management in order to track compliance with training requirements.	No Exceptions Noted.

CC1.0 - Common Criteria Related to the Control Environment (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Employees are required to attend continued training annually that relates to their job, role and responsibilities.	Inspected the Continued Professional Education (CPE) training tracker (or the training completion certificates to determine that employees were required to attend continued training annually that relates to their job role and responsibilities.	No Exceptions Noted.

CC1.0 - Common Criteria Related to the Control Environment (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Personnel are required to read and accept the code of conduct and the statement of confidentiality at the time of hire.	For a sample of new employees, obtained signed code of conduct and statement of confidentiality documents and verified that new personnel are required to read and accept the code of conduct and the statement of confidentiality at the time of hire.	No Exceptions Noted.
		Written job descriptions exist for all key firm personnel and background checks are performed on all new employees.	Inspected written job descriptions for key management and IT personnel to determine whether the job descriptions include responsibilities For a sample of new employees, inspected the results of background checks to determine whether a background check was performed.	
		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.	Obtained the most recent organizational chart and verified through inquiry and observation that Colohouse has developed an organizational structure and reporting lines.	

CC1.0 - Common Criteria Related to the Control Environment (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Senior management meetings are held with key management personnel to discuss the firm's performance and provide oversight of Colohouse's internal control environment.	Obtained documentation relating to senior management meetings and verified that the meetings are held with key management personnel, are documented, and that these meetings discuss the firm's performance and provide oversight of Colohouse's internal control environment.	No Exceptions Noted.

CC2.0 - Common Criteria Related to Communication and Information

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	The IT management system produces information that is timely, current, accurate, complete, accessible, protected, verifiable, and retained in order to support the organization's business activities. 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. Processes are monitored through service level management procedures to help ensure compliance with service level commitments and agreements.	Through inquiry and observation verified that the IT management system produces information that is timely, current, accurate, complete, accessible, protected, verifiable, and retained in order to support Colohouse's business activities. Inspected the information security policies and procedures, an example of job descriptions and the company SharePoint site to determine that organizational and information security policies and procedures were documented for supporting the functioning of controls via the company SharePoint site. Inspected the monitoring and notification systems and an example alert to determine that enterprise monitoring software was utilized to notify personnel when predefined thresholds were exceeded on production systems.	No Exceptions Noted.

C2.0 - Common Criteria Related to Communication and Information (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	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 tool, the antivirus software console, the system monitoring and the firewall rule sets to determine that monitoring software was used to identify and evaluate system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No Exceptions Noted.

C2.0 - Common Criteria Related to Communication and Information (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
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.	Colohouse has developed IT policies and procedures manuals which document 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. 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. Documented escalation procedures for reporting failures incidents, concerns and other complaints are in place and made available to employees through the company intranet.	Inspected the IT policies and procedures manuals to ensure it documents the information that employees need related to security and availability in order to carry out their responsibilities. Inspected communications to internal users regarding update and acknowledgement of IT policies and procedures. Inspected documentation that communicates the security policies to internal users and noted that the communication has provisions for reporting on system complaints and breaches. Inspected the emergency action plan and the entity's SharePoint to determine that documented escalation procedures for reporting failures incidents, concerns and other complaints were in place and made available through the company intranet.	No Exceptions Noted.

C2.0 - Common Criteria Related to Communication and Information (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
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.	All the users who access Colohouse's information systems, are informed and advised of their security obligations and commitments during employee on-boarding, including an acknowledgement of the Colohouse HR and security policies. Colohouse's General Security Procedures mandates that the Data Center Director ensures compliance with applicable regulations and legislations. This policy is communicated to internal users in management meetings or by periodic e-mails to internal authorized users.	For a sample of new hires (employees), inspected the new hire employee acknowledgement forms to determine whether they had signed and acknowledged their review of the employee manual, which includes the security policies, at the time of orientation. Inspected the Colohouse's General Security Procedures and verified that this plan is communicated to internal authorized users.	No Exceptions Noted.

C2.0 - Common Criteria Related to Communication and Information (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
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.	Colohouse provides annual security training for employees and the results are monitored by management in order to track compliance with training requirements. A privacy notice is posted on Colohouse's website. The privacy notice describes the entity's privacy commitments.	Obtained training documentation and verified that annual security training is provided for employees and that the results are monitored by management. Obtained the privacy notice from Colohouse's website and verified that the privacy notice describes the entity's privacy commitments.	No Exceptions Noted.

C2.0 - Common Criteria Related to Communication and Information (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	The entity's objectives, including changes made to the objectives, are communicated to its personnel through the company intranet.	Inspected the entity's SharePoint to determine that the entity's objectives, including changes made to the objectives, were communicated to its personnel through the company intranet.	No Exceptions Noted.
		Management tracks and monitors compliance with training requirements.	Inspected the security awareness training form to determine that management tracked and monitored compliance with information security and awareness training requirements.	
		The entity's third-party agreement delineates the boundaries of the system and describes relevant system components.	Inspected the third-party agreement to determine that the entity's third-party agreement delineated the boundaries of the system and described relevant system components.	

C2.0 - Common Criteria Related to Communication and Information (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	The entity's third-party agreement communicates the system commitments and requirements of third parties.	Inspected the third-party agreement for a sample of third parties to determine that the entity's third-party agreement communicated the system commitments and requirements of third parties.	No Exceptions Noted.

C2.0 - Common Criteria Related to Communication and Information (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	The entity's third-party agreement outlines and communicates the terms, conditions and responsibilities of third parties. Customer responsibilities are outlined and communicated through defined service level agreements (SLA), master service agreements (MSA) and/or the entity website.	Inspected the third-party agreement for a sample of third parties to determine that the entity's third-party agreement outlined and communicated the terms, conditions and responsibilities of third parties. Inspected the agreement for a sample of customers to determine that customer responsibilities were outlined and communicated through defined service level agreements (SLA), master service agreements (MSA) and/or the entity website.	No Exceptions Noted.

C2.0 - Common Criteria Related to Communication and Information (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	Documented escalation procedures for reporting failures incidents, concerns and other complaints are in place and shared with external parties.	Inspected the escalation policies and procedures and the entity's website to determine that documented escalation procedures for reporting failures incidents, concerns and other complaints were in place and shared with external parties.	No Exceptions Noted.
		The entity communicates to external parties, vendors and service providers the system commitments and requirements relating to confidentiality through the use of third-party agreements.	Inspected the third-party agreement for a sample of third parties to determine that the entity communicated to external parties, vendors and service providers the system commitments and requirements relating to confidentiality through the use of third-party agreements.	
		Changes to commitments and requirements relating to confidentiality are communicated to third parties, external users, and customers via e- mail.	Inquired of the operations team regarding changes to commitments and requirements relating to confidentiality to determine that changes to commitments and requirements relating to confidentiality were communicated to third parties, external users and customers via e-mail.	

C2.0 - Common Criteria Related to Communication and Information (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	A privacy notice is posted on Colohouse's website. The privacy notice describes the entity's privacy commitments. Colohouse regularly informs and communicates to external 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.	Obtained the privacy notice from Colohouse's website and verified that the privacy notice describes the entity's privacy commitments. Inspected documentation that communicates the security policies to external users and noted that the communication has provisions for reporting on system complaints and breaches.	No Exceptions Noted.

CC3.0 - Common Criteria Related to Risk Assessment

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	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. 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. Operational and security policies are reviewed and updated, if necessary, on an annual basis.	Obtained and inspected Colohouse strategic plan and verified that Colohouse has developed a strategic plan that identifies key strategic objectives, organization goals, and key performance indicators and allow Colohouse to identify and assess risks that threaten the achievement of these objectives. Inspected the documentation of the risk assessment noting management addressed the operational, financial, and compliance (including fraud assessment) risks and that action plans are developed, if required, to mitigate the risks identified due to these changes. Obtained documentation and verified that the policies are reviewed and updated, if necessary, on an annual basis.	No Exceptions Noted.

CC3.0 - Common Criteria Related to Risk Assessment (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
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.	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. Operational and security policies are reviewed and updated, if necessary, on an annual basis. Data center access is limited to authorized Colohouse employees based on their roles and responsibilities. Access to the data center is approved by data center management.	Inspected the documentation of the risk assessment noting management addressed the operational, financial, and compliance (including fraud assessment) risks and that action plans are developed, if required, to mitigate the risks identified due to these changes. Obtained documentation and verified that the policies are reviewed and updated, if necessary, on an annual basis. Verified that access to the data center is limited to authorized Colohouse employees based on their roles and responsibilities and that access to the data center is approved by data center management.	No Exceptions Noted.

CC3.0 - Common Criteria Related to Risk Assessment (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	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. Operational and security policies are reviewed and updated, if necessary, on an annual basis. Data center access is limited to authorized Colohouse employees based on their roles and responsibilities. Access to the data center is approved by data center management.	Inspected the documentation of the risk assessment noting management addressed the operational, financial, and compliance (including fraud assessment) risks and that action plans are developed, if required, to mitigate the risks identified due to these changes. Obtained documentation and verified that the policies are reviewed and updated, if necessary, on an annual basis. Verified that access to the data center is limited to authorized Colohouse employees based on their roles and responsibilities and that access to the data center is approved by data center management.	No Exceptions Noted.

CC3.0 - Common Criteria Related to Risk Assessment (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	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. Operational and security policies are reviewed and updated, if necessary, on an annual basis. Senior management meetings are held with key management personnel to discuss the firm's performance and provide oversight of Colohouse's internal control environment.	Inspected the documentation of the risk assessment noting management addressed the operational, financial, and compliance (including fraud assessment) risks and that action plans are developed, if required, to mitigate the risks identified due to these changes. Obtained documentation and verified that the policies are reviewed and updated, if necessary, on an annual basis. Obtained documentation relating to senior management meetings and verified that the meetings are held with key management personnel, are documented, and that these meetings discuss the firm's performance and provide oversight of Colohouse's internal control environment.	No Exceptions Noted.

CC4.0 - Common Criteria Related to Monitoring Activities

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
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.	Problems and incidents are documented, tracked, and resolved in a timely manner.	Selected a sample of incidents and verified through the inspection of documentation that incidents were resolved in a timely manner.	No Exceptions Noted.
		Senior management meetings are held with key management personnel to discuss the firm's performance and provide oversight of Colohouse's internal control environment.	Obtained documentation relating to senior management meetings and verified that the meetings are held with key management personnel, are documented, and that these meetings discuss the firm's performance and provide oversight of Colohouse's internal control environment.	
		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 the documentation of the risk assessment noting management addressed the operational, financial, and compliance (including fraud assessment) risks and that action plans are developed, if required, to mitigate the risks identified due to these changes.	

CC4.0 - Common Criteria Related to Monitoring Activities (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
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.	Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. Vulnerability scans are performed annually on the environment to identify control gaps and vulnerabilities.	Inspected the monitoring tool configurations, the antivirus software dashboard console, the system monitoring and the firewall rule sets to determine that software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. Inspected the completed vulnerability scan to determine that vulnerability scans were performed annually on the environment to identify control gaps and vulnerabilities.	No Exceptions Noted.

CC4.0 - Common Criteria Related to Monitoring Activities (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
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.	Problems and incidents are documented, tracked, and resolved in a timely manner.	Selected a sample of incidents and verified through the inspection of documentation that incidents were resolved in a timely manner.	No Exceptions Noted.
		Senior management meetings are held with key management personnel to discuss the firm's performance and provide oversight of Colohouse's internal control environment.	Obtained documentation relating to senior management meetings and verified that the meetings are held with key management personnel, are documented, and that these meetings discuss the firm's performance and provide oversight of Colohouse's internal control environment.	
		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 the documentation of the risk assessment noting management addressed the operational, financial, and compliance (including fraud assessment) risks and that action plans are developed, if required, to mitigate the risks identified due to these changes.	

CC4.0 - Common Criteria Related to Monitoring Activities (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
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.	Senior management is made aware of high-risk vulnerabilities, deviations and controls gaps identified as part of the compliance, control and risk assessments performed. Vulnerability scans are performed annually on the environment to identify control gaps and vulnerabilities.	Inquired of the operations team to determine that senior management was made aware of high-risk vulnerabilities, deviations and controls gaps identified as part of the compliance, control and risk assessments performed. Inspected the completed vulnerability scan to determine that vulnerability scans were performed annually on the environment to identify control gaps and vulnerabilities.	No Exceptions Noted.

CC5.0 - Common Criteria Related to Control Activities

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
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.	Colohouse's security and operational policies are established by senior management of the firm. The policies are developed by the Data Center Directors and approved by management. If any changes are made, an updated document with the new approval date is released to all firm employees. Data center access is limited to authorized Colohouse employees based on their roles and responsibilities. Access to the data center is approved by data center management. 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 the security and operational policies to ascertain whether procedures governing security and availability for the entity are included that contribute to the mitigation of risks to the achievement of objectives to acceptable levels. Verified that access to the data center is limited to authorized Colohouse employees based on their roles and responsibilities and that access to the data center is approved by data center management. Inspected the documentation of the risk assessment noting management addressed the operational, financial, and compliance (including fraud assessment) risks and that action plans are developed, if required, to mitigate the risks identified due to these changes.	No Exceptions Noted.

CC5.0 - Common Criteria Related to Control Activities (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
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.	A disaster recovery plan is developed and updated on an annual basis. The disaster recovery plans is tested on an annual basis.	Inspected the business continuity and disaster recovery plans to determine that a disaster recovery plan was developed and updated on an annual basis. Inspected the completed business continuity and disaster recovery test results to determine that the disaster recovery plans is tested on an annual basis.	No Exceptions Noted.

CC5.0 - Common Criteria Related to Control Activities (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	Colohouse's security and operational policies are established by senior management of the firm. The policies are developed by the Data Center Directors and approved by management. If any changes are made, an updated document with the new approval date is released to all firm employees. Data center access is limited to authorized Colohouse employees based on their roles and responsibilities. Access to the data center is approved by data center management. 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 the security and operational policies to ascertain whether procedures governing security and availability for the entity are included that contribute to the mitigation of risks to the achievement of objectives to acceptable levels. Verified that access to the data center is limited to authorized Colohouse employees based on their roles and responsibilities and that access to the data center is approved by data center management. Inspected the documentation of the risk assessment noting management addressed the operational, financial, and compliance (including fraud assessment) risks and that action plans are developed, if required, to mitigate the risks identified due to these changes.	No Exceptions Noted.

CC5.0 - Common Criteria Related to Control Activities (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	The internal controls implemented around the entity's technology infrastructure include but are not limited to: • Restricting access rights to authorized users • Limiting services to what is required for business operations • Authentication of access Protecting the entity's assets from external threats • Management has established controls around the acquisition, development and maintenance of the entity's technology infrastructure.	Inspected the internal controls matrix to determine that the internal controls implemented around the entity's technology infrastructure included but were not limited to: • Restricting access rights to authorized users • Limiting services to what is required for business operations • Authentication of access • Protecting the entity's assets from external threats Inspected the internal controls matrix to determine that management established controls around the acquisition, development and maintenance of the entity's technology infrastructure.	No Exceptions Noted.

CC5.0 - Common Criteria Related to Control Activities (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	An analysis of incompatible operational duties is performed on at least an annual basis, and where incompatible responsibilities are identified, compensating controls are put into place.	Inspected the organizational chart and the internal controls matrix to determine that an analysis of incompatible operational duties was performed on at least an annual basis, and where incompatible responsibilities were identified, compensating controls were put into place.	No Exceptions Noted.

CC5.0 - Common Criteria Related to Control Activities (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
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.	Colohouse selects and develops general control activities over technology to support the achievement of objectives. These are documented in various policies and programs that address information security, operations, change management, and disaster recovery which are key general controls activities.	Obtained and inspected various policies and plans that address information security, operations, change management, and disaster recovery and verified that Colohouse selects and develops control activities through policies that establish what is expected and in plans that put policies into action. Also verified that the plans assign accountability for performing the control activities, detail the time frame for performing the control, and require that management periodically reviews control activities to determine their continued relevance and refreshes them when necessary.	No Exceptions Noted.

CC5.0 - Common Criteria Related to Control Activities (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
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.	Roles and responsibilities are defined in written job descriptions and communicated to personnel through the company SharePoint site.	Inspected an example of job descriptions and the company intranet to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the company SharePoint site.	No Exceptions Noted.
		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 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.	
		Process owners and management investigate and troubleshoot control failures.	Inspected the completed risk assessment to determine that process owners and management investigated and troubleshot control failures.	

CC6.0 - Common Criteria Related to Logical and Physical Access Controls

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
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.	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. Only authorized users can request changes to data center user access listings. Visitors and contractors are required to sign in and are escorted by authorized personnel when accessing the facility.	Selected a sample of new internal users and determined whether access was authorized and consistent with their role. Selected a sample of terminated internal users and verified access to the systems were removed for these users. Verified through inquiry and observation that only authorized users can request changes to data center user access listings. Verified through inquiry and observation that visitors and contractors are required to sign in and are escorted by authorized personnel when accessing the facility.	No Exceptions Noted.

CC6.0 - Common Criteria Related to Logical and Physical Access Controls (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
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.	Client access lists are configured based on the access control list submitted during the onboarding process. Client access is reviewed periodically by data center management as part of their normal security review procedures (i.e., Single Point of Contact ("SPOC")). There is also a review of data center access performed for employees and vendors as well.	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.
		Administrative access is restricted to appropriate users who require such access to perform their job functions.	Inspected the administrator access listings to determine that administrative access is restricted to appropriate users who require such access to perform their job functions.	
		Alerts are generated to notify administrators of suspicious activity.	Inspected example alerts to determine that alerts were generated to notify administrators of suspicious activity.	
		VPN user access is restricted via role-based security privileges defined within the access control system.	Inspected the VPN user listing to determine that VPN user access was restricted via role-based security privileges defined within the access control system.	

CC6.0 - Common Criteria Related to Logical and Physical Access Controls (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
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.	VPN users are authenticated via username and password. VPN users are authenticated via multifactor authentication. The network, databases, and applications are configured to enforce password requirements that include: - Minimum password length - Minimum password strength - Uppercase letter - Lowercase letter - Numeric characters	Inspected the VPN configurations policy to determine that VPN users were authenticated via username and password. Observed the user login to the VPN to determine that VPN users were authenticated via multifactor authentication. Inspected the network, database, and application password configurations to determine that requirements include the following: - Minimum password length - Minimum password strength - Uppercase letter - Lowercase letter - Numeric characters	No Exceptions Noted.

CC6.0 - Common Criteria Related to Logical and Physical Access Controls (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
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.	Application account lockout settings for the network, databases, and applications are in place that include: - Account lockout duration - Account lockout threshold Account sharing is prohibited by policy.	Inspected the application account lockout settings to determine that application account lockout settings were in place that included: - Account lockout duration - Account lockout threshold Inspected the information security policy to determine that account sharing was prohibited.	No Exceptions Noted.

CC6.0 - Common Criteria Related to Logical and Physical Access Controls (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
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.	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. Only authorized users can request changes to data center user access listings. Visitors and contractors are required to sign in and are escorted by authorized personnel when accessing the facility. Client access lists are configured based on the access control list submitted during the onboarding process. Client access is reviewed periodically by data center management as part of their normal security review procedures (i.e., Single Point of Contact ("SPOC")).	Selected a sample of new internal users and determined whether access was authorized and consistent with their role. Selected a sample of terminated internal users and verified access to the systems were removed for these users. Verified through inquiry and observation that only authorized users can request changes to data center user access listings. Verified through inquiry and observation that visitors and contractors are required to sign in and are escorted by authorized personnel when accessing the facility. 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.

CC6.0 - Common Criteria Related to Logical and Physical Access Controls (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
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.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring. Control self-assessments that include, but are not limited to, physical and logical access reviews, and backup restoration tests are performed on at least an annual basis.	Inspected the information security policies and procedures to determine that documented policies and procedures were in place regarding system settings, authentication, access, and security monitoring. Inquired of the Chief Technology Officer regarding control self-assessments to determine that control self-assessments that included, but were not limited to, physical and logical access reviews, and backup restoration tests were performed on at least an annual basis.	No Exceptions Noted.

CC6.0 - Common Criteria Related to Logical and Physical Access Controls (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
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.	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. Only authorized users can request changes to data center user access listings. Visitors and contractors are required to sign in and are escorted by authorized personnel when accessing the facility. Client access lists are configured based on the access control list submitted during the onboarding process. Client access is reviewed periodically by data center management as part of their normal security review procedures (i.e., Single Point of Contact ("SPOC")).	Selected a sample of new internal users and determined whether access was authorized and consistent with their role. Selected a sample of terminated internal users and verified access to the systems were removed for these users. Verified through inquiry and observation that only authorized users can request changes to data center user access listings. Verified through inquiry and observation that visitors and contractors are required to sign in and are escorted by authorized personnel when accessing the facility. 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.

CC6.0 - Common Criteria Related to Logical and Physical Access Controls (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
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.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring. Control self-assessments that include, but are not limited to, physical and logical access reviews, and backup restoration tests are performed on at least an annual basis.	Inspected the information security policies and procedures to determine that documented policies and procedures were in place regarding system settings, authentication, access, and security monitoring. Inquired of the Chief Technology Officer regarding control self-assessments to determine that control self-assessments that included, but were not limited to, physical and logical access reviews, and backup restoration tests were performed on at least an annual basis.	No Exceptions Noted.

CC6.0 - Common Criteria Related to Logical and Physical Access Controls (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	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.	Observed entrances to the data center and verified that access is restricted using a card key. Obtained a list of personnel with access to the data center, and determined if such access is appropriate for each person based on their job function. Selected a sample of new internal users and determined whether access was authorized and consistent with their role. Selected a sample of terminated internal users and verified access to the systems were removed for these users.	No Exceptions Noted.

CC6.0 - Common Criteria Related to Logical and Physical Access Controls (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	Visitors 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. Surveillance cameras are located at strategic locations within all data centers as a deterrent to unauthorized access.	Through inquiry and observation, verified that 1) visitors must be signed in by an authorized workforce member before a visitor badge can be issued, 2) visitor badges are issued for identification purposes only and do not permit access to any secured areas, and 3) all visitors must be escorted in areas where sensitive system and system components are maintained and operated and that visitors must return their visitor badge at the end of their visit to the security desk. Through inquiry and observation, verified that surveillance cameras are located at strategic locations within all data centers as a deterrent to unauthorized access.	No Exceptions Noted.

CC6.0 - Common Criteria Related to Logical and Physical Access Controls (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	Policies and procedures are in place to guide personnel in physical security activities.	Inspected the physical security policies and procedures to determine that policies and procedures were in place to guide personnel in physical security activities.	No Exceptions Noted.
		A manned reception desk is in place to monitor and control access to the entrance of the office facility during standard business hours.	Observed the entrance to the facility to determine that a manned reception desk was in place to monitor and control access to the entrance of the office facility during standard business hours.	
		A badge access system controls access to and within the office facility.	Observed the presence of badge access points within the facility to determine that a badge access system-controlled access to and within the facility.	
		The sharing of access badges and tailgating are prohibited.	Through inquiry and observation, verified that the sharing of access badges and tailgating are not performed within the production facility.	

CC6.0 - Common Criteria Related to Logical and Physical Access Controls (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	A video surveillance system is in place with footage retained for 90 days. Visitors to the facility and server room are required to sign a visitor log prior upon arrival. User access to the badge access system is reviewed on an annual basis.	Inspected the video surveillance system configurations and oldest retained video surveillance footage to determine that a video surveillance system was in place with footage retained for 90 days. Inspected an example visitor log to determine that visitors to the facility and server room were required to sign a visitor log prior upon arrival. Inspected the completed badge access review to determine that user access to the badge access system was reviewed on an annual basis.	No Exceptions Noted.

CC6.0 - Common Criteria Related to Logical and Physical Access Controls (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
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.	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. Policies and procedures are in place to guide personnel in data, hardware and software disposal and destruction. The entity purges data stored on backup tapes and backup drives upon customer cancellation request.	Selected a sample of new internal users and determined whether access was authorized and consistent with their role. Selected a sample of terminated internal users and verified access to the systems were removed for these users. Inspected the data disposal and destruction policies and procedures to determine that policies and procedures were in place to guide personnel in data, hardware and software disposal and destruction. Inspected an example supporting service cancellation ticket for a customer cancellation request to determine that the entity purged data stored on backup tapes and backup drives upon customer cancellation request.	No Exceptions Noted.

CC6.0 - Common Criteria Related to Logical and Physical Access Controls (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
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.	Data that is no longer required for business purposes is rendered unreadable.	Inspected the data disposal and destruction policies and procedures to determine that data that was no longer required for business purposes was rendered unreadable.	No Exceptions Noted.

CC6.0 - Common Criteria Related to Logical and Physical Access Controls (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Network address translation (NAT) functionality is utilized to manage internal IP addresses. VPN, SSL, secure file transfer program (SFTP), and other encryption technologies are used for defined points of connectivity. VPN user access is restricted via role-based security privileges defined within the access control system.	Inspected the NAT configurations to determine that NAT functionality was utilized to manage internal IP addresses. Inspected the encryption configurations, the VPN authentication configurations and the digital certificates to determine that VPN, SSL, secure file transfer program (SFTP), and other encryption technologies were used for defined points of connectivity. 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.

CC6.0 - Common Criteria Related to Logical and Physical Access Controls (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	VPN users are authenticated via username and password.	Inspected the VPN configurations policy to determine that VPN users were authenticated via username and password.	No Exceptions Noted.
		VPN users are authenticated via multifactor authentication.	Observed the user login to the VPN to determine that VPN users were authenticated via multifactor authentication.	
		Server certificate-based authentication is used as part of the SSL/TLS encryption with a trusted certificate authority.	Inspected the encryption configurations for data in transit and digital certificates to determine that server certificate-based authentication was used as part of the SSL/TLS encryption with a trusted certificate authority.	
		Transmission of digital output beyond the boundary of the system is encrypted.	Inspected the encryption configurations for data in transit and digital certificates to determine that transmission of digital output beyond the boundary of the system was encrypted.	

CC6.0 - Common Criteria Related to Logical and Physical Access Controls (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	A firewall is in place to filter unauthorized inbound network traffic from the internet. The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the network diagram and the firewall rulesets to determine that a firewall was in place to filter unauthorized inbound network traffic from the internet. Inspected the network diagram and the firewall rulesets to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No Exceptions Noted.

CC6.0 - Common Criteria Related to Logical and Physical Access Controls (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
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.	Use of removable media is prohibited by policy except when authorized by management. The ability to recall backed up data is restricted to authorized personnel. The entity secures its environment using a multi-layered defense approach that includes firewalls and antivirus software.	Inspected information security policies and procedures to determine that the use of removable media was prohibited by policy except when authorized by management. Inspected the list of users with the ability to recall backup media from the third-party storage facility to determine that the ability to recall backed up data was restricted to authorized personnel. Inspected the network diagram, the firewall rule sets and the antivirus settings to determine that the entity secures its environment using a multi-layered defense approach that included firewalls and antivirus software.	No Exceptions Noted.

CC6.0 - Common Criteria Related to Logical and Physical Access Controls (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
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.	VPN, SSL, secure file transfer program (SFTP), and other encryption technologies are used for defined points of connectivity.	Inspected the encryption configurations, the VPN authentication configurations and the digital certificates to determine that VPN, SSL, secure file transfer program (SFTP), and other encryption technologies were used for defined points of connectivity.	No Exceptions Noted.
		Server certificate-based authentication is used as part of the SSL/TLS encryption with a trusted certificate authority.	Inspected the encryption configurations for data in transit and digital certificates to determine that server certificate-based authentication was used as part of the SSL/TLS encryption with a trusted certificate authority.	
		Backup media is stored in an encrypted format.	Inspected the backup encryption settings to determine that backup media was stored in an encrypted format.	

CC6.0 - Common Criteria Related to Logical and Physical Access Controls (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
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.	Transmission of digital output beyond the boundary of the system is encrypted.	Inspected the encryption configurations for data in transit and digital certificates to determine that transmission of digital output beyond the boundary of the system was encrypted.	No Exceptions Noted.

CC6.0 - Common Criteria Related to Logical and Physical Access Controls (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
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.	Documented change control policies and procedures are in place to guide personnel in the change management process.	Inspected the change management policies and procedures to determine that documented change control policies and procedures were in place to guide personnel in the change management process.	No Exceptions Noted.
		Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	Inspected the antivirus software settings to determine that antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained 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 antivirus software settings to determine that the antivirus software provider pushed updates to the installed antivirus software as new updates/signatures were available.	

CC6.0 - Common Criteria Related to Logical and Physical Access Controls (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
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.	The antivirus software is configured to scan workstations on a periodic basis.	Inspected the antivirus scan settings to determine that the antivirus software was configured to scan workstations on a periodic basis.	No Exceptions Noted.

CC7.0 - Common Criteria Related to System Operations

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
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.	Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment. 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 the security and operational policies to ascertain whether procedures governing the detection, logging, and monitoring of unknown or unauthorized components into the environment are in place. Inspected system documentation and verified that monitoring software and network hardware (i.e., firewalls) are in place to monitor system security, vulnerabilities, and changes that are made to the system.	No Exceptions Noted.

CC7.0 - Common Criteria Related to System Operations (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
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.	Management has defined configuration standards in the information security policies and procedures. Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. The monitoring software is configured to alert appropriate personnel when thresholds have been exceeded.	Inspected the information security policies and procedures to determine that management had defined configuration standards in the information security policies and procedures. Inspected the monitoring tool configurations, the antivirus software dashboard console, the system monitoring configurations and the firewall rule sets to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. Inspected the monitoring and notification systems and an example alert to determine that enterprise monitoring software was utilized to notify personnel when predefined thresholds were exceeded on production systems.	No Exceptions Noted.

CC7.0 - Common Criteria Related to System Operations (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
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.	Use of removable media is prohibited by policy except when authorized by management. A firewall is in place to filter unauthorized inbound network traffic from the internet.	Inspected the information security policies and procedures to determine that the use of removable media was prohibited by policy except when authorized by management. Inspected the network diagram and the firewall rulesets to determine that a firewall was in place to filter unauthorized inbound network traffic from the internet.	No Exceptions Noted.

CC7.0 - Common Criteria Related to System Operations (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
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.	Problems and incidents are documented, tracked, and resolved in a timely manner. Senior management meetings are held with key management personnel to discuss the firm's performance and provide oversight of Colohouse's internal control environment. Environmental systems are monitored and issues related to environmental equipment are documented and resolved timely by network operations center ("NOC") personnel.	Selected a sample of incidents and verified through the inspection of documentation that incidents were resolved in a timely manner. Obtained documentation relating to senior management meetings and verified that the meetings are held with key management personnel, are documented, and that these meetings discuss the firm's performance and provide oversight of Colohouse's internal control environment. Through inquiry and observation, verified that environmental systems are monitored and issues related to environmental equipment are documented and resolved timely by NOC personnel.	No Exceptions Noted.

CC7.0 - Common Criteria Related to System Operations (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
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.	Internal and external vulnerability scans and penetration tests are performed on at least an annual basis and remedial actions are taken where necessary.	Inspected the completed vulnerability scan results and the completed penetration test results to determine that internal and external vulnerability scans and penetration tests were performed on at least an annual basis and remedial actions were taken where necessary.	No Exceptions Noted.
		Documented incident response policies and procedures are in place to guide personnel in the event of an incident.	Inspected the emergency action plan to determine that documented incident response policies and procedures were in place to guide personnel in the event of an incident.	
		Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	Inspected the information security policy and the emergency action plan to determine that policies and procedures were in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	

CC7.0 - Common Criteria Related to System Operations (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
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.	The monitoring software is configured to alert appropriate personnel when thresholds have been exceeded.	Inspected the monitoring and notification systems and an example alert to determine that enterprise monitoring software was utilized to notify personnel when predefined thresholds were exceeded on production systems.	No Exceptions Noted.

CC7.0 - Common Criteria Related to System Operations (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
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.	Problems and incidents are documented, tracked, and resolved in a timely manner.	Selected a sample of incidents and verified through the inspection of documentation that incidents were recorded and tracked on an incident ticket and resolved in a timely manner.	No Exceptions Noted.
		Senior management meetings are held with key management personnel to discuss the firm's performance and provide oversight of Colohouse's internal control environment.	Obtained documentation relating to senior management meetings and verified that the meetings are held with key management personnel, are documented, and that these meetings discuss the firm's performance and provide oversight of Colohouse's internal control environment.	
		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 the documentation of the risk assessment noting management addressed the operational, financial, and compliance (including fraud assessment) risks and that action plans are developed, if required, to mitigate the risks identified due to these changes.	

CC7.0 - Common Criteria Related to System Operations (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
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.	Environmental systems are monitored and issues related to environmental equipment are documented and resolved timely by NOC personnel.	Through inquiry and observation, verified that environmental systems are monitored and issues related to environmental equipment are documented and resolved timely by NOC personnel.	No Exceptions Noted.
		Documented incident response policies and procedures are in place to guide personnel in the event of an incident.	Inspected the emergency action plan to determine that documented incident response policies and procedures were in place to guide personnel in the event of an incident.	
		The incident response and escalation procedures are reviewed at least annually for effectiveness.	Inspected the emergency action plan to determine that the incident response and escalation procedures were reviewed at least annually for effectiveness.	
		Incidents resulting in the unauthorized use or disclosure of personal information are communicated to the affected users.	Inquired of the Data Center Operations personnel regarding security incidents to determine that incidents resulting in the unauthorized use or disclosure of personal information were identified and communicated to the affected users.	

CC7.0 - Common Criteria Related to System Operations (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
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.	Problems and incidents are documented, tracked, and resolved in a timely manner.	Selected a sample of incidents and verified through the inspection of documentation that incidents were recorded and tracked on an incident ticket and resolved in a timely manner.	No Exceptions Noted.
		Senior management meetings are held with key management personnel to discuss the firm's performance and provide oversight of Colohouse's internal control environment.	Obtained documentation relating to senior management meetings and verified that the meetings are held with key management personnel, are documented, and that these meetings discuss the firm's performance and provide oversight of Colohouse's internal control environment.	
		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 the documentation of the risk assessment noting management addressed the operational, financial, and compliance (including fraud assessment) risks and that action plans are developed, if required, to mitigate the risks identified due to these changes.	

CC7.0 - Common Criteria Related to System Operations (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
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.	Environmental systems are monitored and issues related to environmental equipment are documented and resolved timely by NOC personnel.	Through inquiry and observation, verified that environmental systems are monitored and issues related to environmental equipment are documented and resolved timely by NOC personnel.	No Exceptions Noted.
		Documented incident response policies and procedures are in place to guide personnel in the event of an incident.	Inspected the emergency action plan to determine that documented incident response policies and procedures were in place to guide personnel in the event of an incident.	
		The incident response and escalation procedures are reviewed at least annually for effectiveness.	Inspected the emergency action plan to determine that the incident response and escalation procedures were reviewed at least annually for effectiveness.	
		Incidents resulting in the unauthorized use or disclosure of personal information are communicated to the affected users.	Inquired of the Data Center Operations personnel regarding security incidents to determine that incidents resulting in the unauthorized use or disclosure of personal information were identified and communicated to the affected users.	

CC7.0 - Common Criteria Related to System Operations (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Problems and incidents are documented, tracked, and resolved in a timely manner.	Selected a sample of incidents and verified through the inspection of documentation that incidents were recorded and tracked on an incident ticket and resolved in a timely manner.	No Exceptions Noted.
		Senior management meetings are held with key management personnel to discuss the firm's performance and provide oversight of Colohouse's internal control environment.	Obtained documentation relating to senior management meetings and verified that the meetings are held with key management personnel, are documented, and that these meetings discuss the firm's performance and provide oversight of Colohouse's internal control environment.	
		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 the documentation of the risk assessment noting management addressed the operational, financial, and compliance (including fraud assessment) risks and that action plans are developed, if required, to mitigate the risks identified due to these changes.	

CC7.0 - Common Criteria Related to System Operations (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Environmental systems are monitored and issues related to environmental equipment are documented and resolved timely by NOC personnel.	Through inquiry and observation, verified that environmental systems are monitored and issues related to environmental equipment are documented and resolved timely by NOC personnel.	No Exceptions Noted.
		Documented incident response policies and procedures are in place to guide personnel in the event of an incident.	Inspected the emergency action plan to determine that documented incident response policies and procedures were in place to guide personnel in the event of an incident.	
		The incident response and escalation procedures are reviewed at least annually for effectiveness.	Inspected the emergency action plan to determine that the incident response and escalation procedures were reviewed at least annually for effectiveness.	
		Incidents resulting in the unauthorized use or disclosure of personal information are communicated to the affected users.	Inquired of the Data Center Operations personnel regarding security incidents to determine that incidents resulting in the unauthorized use or disclosure of personal information were identified and communicated to the affected users.	

CC7.0 - Common Criteria Related to System Operations (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	A disaster recovery plan is documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.	Inspected the business continuity and disaster recovery plans to determine that a disaster recovery plan was documented to identify and reduce risks, limited the consequences of damaging incidents, and ensured the timely resumption of essential operations.	No Exceptions Noted.
		A disaster recovery plan is developed and updated on an annual basis.	Inspected the business continuity and disaster recovery plans to determine that a disaster recovery plan was developed and updated on an annual basis.	
		The disaster recovery plans is tested on an annual basis.	Inspected the completed business continuity and disaster recovery test results to determine that the disaster recovery plans is tested on an annual basis.	

CC8.0 - Common Criteria Related to Change Management

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
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.	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. Senior management meetings are held with key management personnel to discuss the firm's performance and provide oversight of Colohouse's internal control environment. 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.	Inspected the change management policies to determine whether procedures are documented to include a provision that 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. Obtained documentation from a recent weekly management meeting and verified that the meetings discuss any operating issues and incidents. Obtained data center access listings for Colohouse personnel and an example client and verified that 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.	No Exceptions Noted.

CC8.0 - Common Criteria Related to Change Management (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
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.	Documented change control policies and procedures are in place to guide personnel in the handling system changes. Access to implement changes in the production environment is restricted to authorized personnel. System changes are authorized and approved by management prior to implementation.	Inspected the development policy to determine that documented change control procedures were in place to guide personnel in the handling of system changes. Inspected the list of users with access to deploy changes into the production environment to determine that access to implement changes in the production environment was restricted to authorized personnel. Inspected the supporting change tickets for a sample of infrastructure and application changes to determine that system changes were authorized and approved by management prior to implementation.	No Exceptions Noted.

CC8.0 - Common Criteria Related to Change Management (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
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.	Development and test environments are physically and logically separated from the production environment.	Inspected the separate development, QA and production environments to determine that development and test environments were physically and logically separated from the production environment.	No Exceptions Noted.
		System change requests are documented and tracked in a ticketing system.	Inspected the supporting change tickets for a sample of infrastructure and application changes to determine that system change requests were documented and tracked in a ticketing system.	
		System changes are tested prior to implementation. Types of testing performed depend on the nature of the change.	Inspected the supporting change tickets for a sample of infrastructure and application changes to determine that system changes were tested prior to implementation and that types of testing performed depended on the nature of the change.	

CC8.0 - Common Criteria Related to Change Management (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
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.	Information security policies and procedures document the baseline requirements for configuration of IT systems and tools. Documented change control policies and procedures are in place to guide personnel in implementing changes in an emergency situation.	Inspected the information security policies and procedures to determine that information security policies and procedures documented the baseline requirements for configuration of IT systems and tools. Inspected the development policy to determine that documented change control policies and procedures were in place to guide personnel in implementing changes in an emergency situation.	No Exceptions Noted.

CC9.0 - Common Criteria Related to Risk Mitigation

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Colohouse has developed a disaster recovery plan that identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions. 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. 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.	Obtained and inspected the disaster recovery plan and verified that it identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions. Inspected the risk assessment policy to determine that management defined a formal risk assessment process that specified the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances. Inspected the completed risk assessment to determine that a formal risk assessment was performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	No Exceptions Noted.

CC9.0 - Common Criteria Related to Risk Mitigation (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Identified risks are rated using a risk evaluation process and ratings are approved by management.	Inspected the risk assessment policy and the completed risk assessment to determine that identified risks were rated using a risk evaluation process and ratings were approved by management.	No Exceptions Noted.

CC9.0 - Common Criteria Related to Risk Mitigation (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Colohouse has developed a data center management policy and plan that assesses and manages risks associated with vendors and business partners. 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.	BT obtained and inspected the data center management policy and plan and verified that it assesses and manages risks associated with vendors and business partners. Selected a sample of new customers/vendors and verified that confidentiality agreements applicable to that entity were in place and/or updated and acknowledged by both the entity and Colohouse. Inspected the vendor management policy to determine that management 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.

CC9.0 - Common Criteria Related to Risk Mitigation (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Management develops third-party risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the vendor management policy and the completed vendor risk assessment to determine that management developed third-party risk mitigation strategies to address risks identified during the third-party risk assessment process.	No Exceptions Noted.
		Identified third-party risks are rated using a risk evaluation process and ratings are approved by management.	Inspected the vendor management policy and the completed vendor risk assessment to determine that identified third-party risks were rated using a risk evaluation process and ratings are approved by management.	

Additional Criteria for Availability

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
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.	Environmental systems are monitored and issues related to environmental equipment are documented and resolved timely. Management performs weekly management meetings to discuss operating issues and incidents. 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.	Verified through inquiry and observation that environmental systems are monitored and issues related to environmental equipment are documented and resolved timely. Obtained documentation from a recent weekly management meeting and verified that the meetings discuss any operating issues and incidents. Obtained documentation from a recent maintenance project and verified that 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.	No Exceptions Noted.

Additional Criteria for Availability (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
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.	Enterprise monitoring software is utilized to notify personnel when predefined thresholds are exceeded on production systems.	Inspected the monitoring and notification systems and an example alert to determine that enterprise monitoring software was utilized to notify personnel when predefined thresholds were exceeded on production systems.	No Exceptions Noted.
		The monitoring software is configured to alert IT personnel when thresholds have been exceeded.	Inspected an example alert generated notification to determine that the monitoring software was configured to alert IT personnel when thresholds were exceeded.	
		Processing capacity is monitored 24x7x365.	Inspected the monitoring tool configurations to determine that processing capacity was monitored 24x7x365.	

Additional Criteria for Availability (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	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	Verified through inquiry and observation that environmental controls such as air conditioning, fire suppression, adequate lighting, power distribution units, generators, and an uninterruptible power supply are in place in the data centers to provide for the proper level of environmental controls.	No Exceptions Noted.
		Environmental systems are monitored and issues related to environmental equipment are documented and resolved timely.	Verified through inquiry and observation that environmental systems are monitored and issues related to environmental equipment are documented and resolved timely.	
		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.	Obtained the business continuity plan and disaster recovery plan and verified that plans are in place to guide personnel in the decisions, responsibilities and requirements following disruptions to services and operations.	

Additional Criteria for Availability (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	Disaster recovery testing is performed on an annual basis and the test results are reviewed and the contingency plan is adjusted as needed. Environmental threats that could impair the availability of the system are considered and identified as a part of the risk assessment process. Enterprise monitoring software is utilized to notify personnel when predefined thresholds are exceeded on production systems.	Through inquiry and inspection of documentation, verified that disaster recovery testing is performed on an annual basis and that test results are reviewed and the contingency plan is adjusted as needed on production systems. Inspected the completed risk assessment to determine that environmental threats that could impair the availability of the system were considered and identified as a part of the risk assessment process. Inspected the monitoring and notification systems and an example alert to determine that enterprise monitoring software was utilized to notify personnel when predefined thresholds were exceeded on production systems.	No Exceptions Noted.

Additional Criteria for Availability (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	Production equipment within the colocation areas of the data center facilities is placed on racks to protect infrastructure from localized flooding. Some data center facilities are equipped with raised flooring to elevate equipment and help facilitate cooling. The data center facilities are equipped with leak detection systems to detect water in the event of a flood or water leakage.	Observed the racks housing the equipment to determine that production equipment within the colocation areas of the data center facilities was placed on racks to protect infrastructure from localized flooding. Observed the raised floors within the colocation center to determine that the data center facilities were equipped with raised flooring to elevate equipment and help facilitate cooling. Observed the leak detection devices to determine that the data center facilities were equipped with leak detection systems to detect water in the event of a flood or water leakage.	No Exceptions Noted.

Additional Criteria for Availability (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	IT personnel monitor the success or failure of backups, and are notified of backup job status via e-mail notifications. Restore tests are performed on backed up data upon notification of a failed backup job. Backup media is stored in an encrypted format.	Inspected the backup notification configurations and an example backup status alert to determine that IT personnel monitored the success or failure of backups, and were notified of backup job status via e-mail notifications. Inspected an example backup restore to determine that restore tests were performed on backed up data upon notification of a failed backup job. Inspected the backup encryption settings to determine that backup media was stored in an encrypted format.	No Exceptions Noted.

Additional Criteria for Availability (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	The ability to recall backed up data is restricted to authorized personnel.	Inspected the list of users with the ability to recall backup media from the third-party storage facility to determine that the ability to recall backed up data was restricted to authorized personnel.	No Exceptions Noted.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	A disaster recovery plan is documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations. A disaster recovery plan is developed and updated on an annual basis.	Inspected the business continuity and disaster recovery plans to determine that a disaster recovery plan was documented to identify and reduce risks, limited the consequences of damaging incidents, and ensured the timely resumption of essential operations. Inspected the business continuity and disaster recovery plans to determine that a disaster recovery plan was developed and updated on an annual basis.	No Exceptions Noted.

Additional Criteria for Availability (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	The disaster recovery plans are tested on an annual basis. Data backup restoration tests on at least an annual basis.	Inspected the completed business continuity and disaster recovery test results to determine that the disaster recovery plans are tested on an annual basis. Inspected the completed backup restoration test results for a sample of days to determine that data backup restorations were performed on at least an annual basis.	No Exceptions Noted.

Additional Criteria for Confidentiality

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	Documented confidential policies and procedures are in place that include the following: • Defining, identifying and designating information as confidential. • Storing confidential information. • Protecting confidential - information from erasure or destruction. • Retaining confidential information for only as long as is required to achieve the purpose for which the data was collected and processed. An inventory log is maintained of assets with confidential data.	Inspected the confidentiality policies and procedures to determine that documented confidential policies and procedures were in place that included: • Defining, identifying and designating information as confidential. • Storing confidential information. • Protecting confidential information from erasure or destruction. • Retaining confidential information for only as long as is required to achieve the purpose for which the data was collected and processed. Inspected the master list of system components to determine that an inventory log was maintained of assets with confidential data.	No Exceptions Noted.

Additional Criteria for Confidentiality (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	Confidential information is maintained in locations restricted to those authorized to access.	Inquired of the Chief Technology Officer regarding confidential information to determine that confidential information was maintained in locations restricted to those authorized to access. Inspected the file access permissions and development tracking for confidential information to determine that confidential information was maintained in locations restricted to those authorized to access.	No Exceptions Noted.

Additional Criteria for Confidentiality (continued)

Ref. #	Trust Services Category	Controls Specified by Colohouse	Tests Performed by Service Auditor	Results of Testing
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	Documented data destruction policies and procedures are in place that include the following: • Identifying confidential information requiring destruction when the end of the retention period is reached. • Erasing or destroying confidential information that has been identified for destruction.	Inspected the data disposal and destruction policies and procedures to determine that documented data destruction policies and procedures were in place that included: • Identifying confidential information requiring destruction when the end of the retention period is reached. • Erasing or destroying confidential information that has been identified for destruction. Inspected an example service cancellation ticket for a customer cancellation request to determine that data that was no longer required for business purposes was rendered unreadable.	No Exceptions Noted.