Connectria, LLC

Ontario Securities Act Compliance (Bill 198)

CSAE 3416 Type II Independent Report on a Description of a Service Organization's System and the Suitability of the Design and Operating Effectiveness of the Controls for the period of October 1, 2019, through September 30, 2020.

Using CSAE 3000, Attestation Engagements Other than Audits or Reviews of Historical Information

KirkpatrickPrice

4235 Hillsboro Pike
Suite 300
Nashville, TN 37215

TABLE OF CONTENTS

SECTION I:
INDEPENDENT SERVICE AUDITOR'S REPORT

on Connectria, LLC's Description of Its Managed Services System and the Suitability of the Design and Operating Effectiveness of the Controls

Richard S. Waidmann
CEO
Connectria, LLC
10845 Olive Blvd, Ste 300
Saint Louis, MO 63141

Scope

We have examined Connectria, LLC's description of its managed services system, documented in Section III, for hosting user entities' networks and data throughout the period of October 1, 2019, to September 30, 2020. The examination evaluated the suitability of the design and operating effectiveness of the included controls to achieve the related control objectives stated in the description, based on the criteria identified in Section II. The controls and control objectives included in the description are those that management of Connectria, LLC believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the managed services system that are not likely to be relevant to user entities' internal control over financial reporting. These controls and control objectives have been placed into operation to aid clients' compliance efforts with the requirements in the Ontario Securities Act (Bill 198).

Due to the global pandemic declared by the World Health Organization on March 11, 2020, physical and environmental controls could not be tested; instead, controls were corroborated through remote inspection of related systems and tools.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of Connectria, LLC's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Connectria, LLC uses Netrality Properties, CyrusOne, 365 Data Centers, and Equinix for data center services, Iron Mountain for backup and tape storage, and Wasabi for offsite backups. The description includes only the control objectives and related controls of Connectria, LLC and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified by Connectria, LLC can be achieved only if complementary subservice organization controls assumed in the design of Connectria, LLC's controls are suitably designed and operating effectively, along with the related controls at Connectria, LLC. Our examination did not extend to controls of the subservice organizations, and we have not evaluated the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

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

Service Auditor's Responsibilities

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

Our examination was conducted in accordance with attestation standards established by the Canadian Standard on Assurance Engagements for Reporting on Controls at a Service Organization, set out in the CPA Canada Guide. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period of October 1, 2019, to September 30, 2020. 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 of controls involves

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in hosting networks and data. Also, the projection to the

future of any suitability of the design of the controls to achieve the related control objectives, is subject to the risk that controls at a service organization may become ineffective.

Opinion

In our opinion, in all material respects, based on the criteria described in Connectria, LLC's assertion

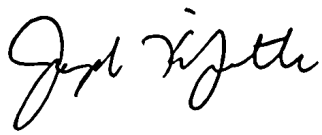
a. the description fairly presents the managed services system that was designed and implemented throughout the period of October 1, 2019, to September 30, 2020.

b. the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period October 1, 2019, to September 30, 2020, and subservice organizations and user entities applied the complementary controls assumed in the design of Connectria, LLC's controls throughout the period of October 1, 2019, to September 30, 2020.

c. the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period of October 1, 2019, to September 30, 2020, if complementary subservice organization and user entity controls assumed in the design of Connectria, LLC's controls operated effectively throughout the period of October 1, 2019, to September 30, 2020.

Restricted Use

This report is intended solely for the information and use of management of Connectria, LLC, user entities of Connectria, LLC's managed services system throughout the period of October 1, 2019, to September 30, 2020, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than the specified parties.



Joseph Kirkpatrick
CPA, CISSP, CGEIT, CISA, CRISC, QSA
4235 Hillsboro Pike, Suite 300
Nashville, TN 37215

November 13, 2020

SECTION II:
CONNECTRIA, LLC'S ASSERTION

CONNECTRIA, LLC'S ASSERTION

We have prepared the description of Connectria, LLC's managed services system entitled, "Connectria, LLC's Description of Its Managed Services System," for hosting user entities' networks and data throughout the period October 1, 2019, to September 30, 2020, for user entities of the system during some or all of the period October 1, 2019, to September 30, 2020, and their auditors who audit and report on such user entities' financial statements or internal controls over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by subservice organizations and user entities themselves, when obtaining an understanding of user entities' information and communication systems relevant to financial reporting. These controls and related control objectives have been placed into operation to aid clients' compliance efforts with the Ontario Securities Act (Bill 198).

Connectria, LLC uses Netrality Properties, CyrusOne, 365 Data Centers, and Equinix for data center services, Iron Mountain for backup and tape storage, and Wasabi for offsite backups. The description includes only the control objectives and related controls of Connectria, LLC and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified in the description can be achieved only if complementary subservice organization controls assumed in the design of our controls are suitably designed and operating effectively, along with the related controls. The description does not extend to controls of the subservice organizations.

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

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

a. the description fairly presents the managed services system made available to user entities of the system during some or all of the period October 1, 2019, to September 30, 2020, for hosting networks and data as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description

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

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

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

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

4) how the system captures and addressed significant events and conditions other than transactions.

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

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

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

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

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

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

b. the controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period October 1, 2019, to September 30, 2020, to achieve those control objectives if subservice organizations and user entities applied the complementary controls assumed in the design of Connectria, LLC's controls throughout the period of October 1, 2019, to September 30, 2020. The criteria we used in making this assertion were that

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

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

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

SECTION III:
CONNECTRIA, LLC'S DESCRIPTION OF ITS SYSTEM

OVERVIEW OF SERVICES PROVIDED

Located in St. Louis, Missouri, Connectria, LLC (Connectria) provides hosting solutions, which address various client needs, including Software as a Service (SaaS), Desktop as a Service (DaaS), Infrastructure as a Service (IaaS), and compliance hosting, such as Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standards (PCI DSS), and disaster recovery across a wide range of platforms. Additional services include application hosting, whether pre-packaged or custom, as well as other data center outsourcing services. Services provided include the following:

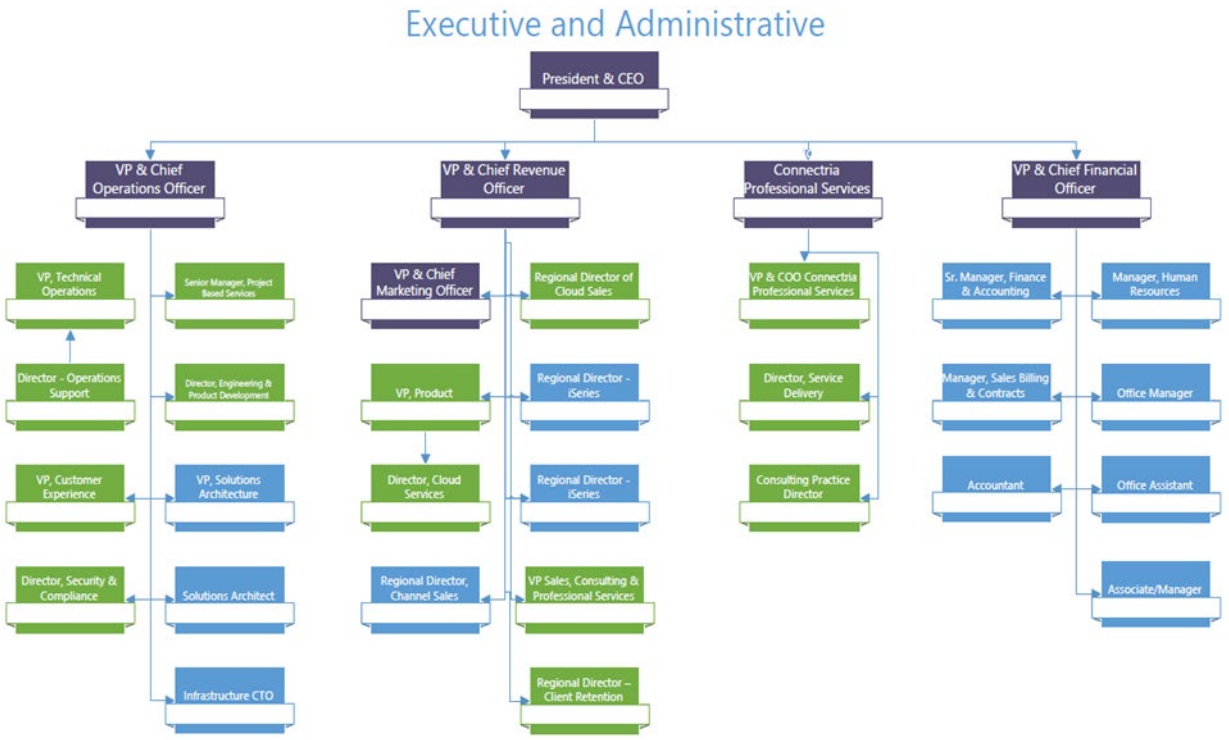
- Managed Hosting – Provides administration, management, and support of client environments
- Managed Cloud – Tailors cloud solutions for public, private, hybrid, or multi-cloud environments
- Managed Services – Includes monitoring for errors and alerts, performance monitoring, and database administration
- Security and Compliance – Ongoing compliance monitoring for PCI, HIPAA, and other security frameworks

Connectria is a data center facility and managed services provider that supports its customers by providing the following services:

- Dedicated hardware and software procurement
- Engineering and implementation services
- 24/7 staffed network operations center
- 24/7 monitoring and escalation services
- System administration services
- Problem determination/resolution
- Operating system upgrades and patching
- Database administration services
- Data backup and restore services with offsite tape storage
- Redundant internet connectivity
- Managed firewall services
- Routing, switching, and load balancing
- Change management
- Trouble ticket system access

Organization

Connectria maintains an appropriate organizational structure that is separated into distinct, functional areas to ensure business efficiency and segregation of duties. An organization chart, pictured below, is maintained to document the defined corporate structure, including established leadership, reporting lines, and a separation of duties.



Additionally, Connectria has appointed a Board of Directors that provides general oversight for the organization. The board members are composed of corporate leadership and external personnel with industry expertise. Per Connectria's Limited Liability Company Agreement, holding company members act through meetings and written consents, and each member is entitled to vote based on their percentage of ownership of the voting units.

Management Control

Management regularly communicates with personnel and enforces the use of the Employee Handbook and training to set the tone and direction for the company. Connectria management primarily communicates via email and newsletter distribution, and the organization maintains an internal Confluence page to communicate policy and procedure to all employees. Training is conducted on an annual basis to ensure personnel are aware of their security responsibilities and procedures.

The organization has a process in place for creating, approving, and updating policies and documentation. Per the Security Program document, Connectria's management team is

responsible for maintaining documentation and ensuring compliance. The Security Program is reviewed and revised, if necessary, on an annual basis, and older policies are retained indefinitely for reference. The critical policies and documents in place include the following:

- Access Control Policy
- Antivirus/Malware Policy
- Asset Management Policy
- Backup and Recovery Policy
- Border Router Configuration Policy
- Browser Configuration Policy
- Business Associate Agreement
- Change Management Policy
- Compliance Policy
- Configuration Standards
- Connectria Charter
- Contract Management Policy
- Cryptographic Key Management Policy
- Data Classification/Ownership Policy
- Data Destruction Policy
- Electronic Messaging Policy
- Elevated Account Policy
- Employee New Hire Template
- Encryption and Hashing Policy
- Encryption Key Management Policy
- Firewall Configuration Policy
- Firewall Router Configuration Policy
- Hardening Standards
- IDS/IPS Configuration Policy
- Incident Response Plan
- Incident Response Procedures
- Internal Router Configuration Policy
- Logging and Monitoring Policy
- Maintenance Policy
- Master Services Agreement
- Multi-Factor Authentication Policy
- Network Diagram
- Network Methodology Testing Policy
- Network Segmentation Policy
- NOC End of Shift Reports
- Onboarding Policy
- OS Hardening Policy
- Password Policy
- Patch Management Policy
- Patching Procedures
- Penetration Testing
- Physical Security Policy
- Project Management Policy
- Remote Access Policy
- Risk Assessment Policy
- Risk Assessment Process
- Security Awareness
- Security Program
- Service Accounts Policy
- SOC Shift Task Lists
- Software Approval Policy
- SQL Server Policy
- Systems Usage Agreement
- Termination Policy
- User Account Policy
- Vendor Management Policy
- Vendor Risk Assessment Policy
- Visitor Policy
- Vulnerability Management Policy
- Vulnerability Scanning Procedure

In addition, Connectria maintains contractual agreements and a website that define the scope of services provided to its clients. Master service agreements, statements of work, non-disclosure agreements, and business associate agreements are structured to provide clarity in roles and expectations and to support the business by providing clear details of relevant services, expectations, and limits. The contracts and agreements define the responsibilities of internal personnel to ensure that they are aware of their responsibilities to clients.

Integrity and Ethics

Management oversees the communication and implementation of Connectria's Code of Conduct. The Code of Conduct is communicated via the Employee Handbook, the Systems Usage Agreement, and the Confidentiality Agreement, which require acknowledgements by personnel during orientation and annually thereafter. The Employee Handbook is available for review on Connectria's paycheck site. Human Resources (HR) communicates changes or updates to the Code of Conduct via Connectria's internal intranet/blog site.

Controls Related to Personnel

Job Descriptions

Connectria maintains formal job descriptions for all critical functions within the organization to ensure that employees are aware of their roles and responsibilities. The descriptions include sections that address primary responsibilities, qualifications and experience, and preferred skills. Job descriptions are used when recruiting and assigning access to personnel.

Hiring, Termination, and Personnel Changes

During the pre-hire phase, the organization conducts testing and background checks. Potential hires undergo a series of interviews, and skills testing is completed by those applying for technical positions. HR uses Sterling Talent Solutions to conduct criminal and financial background checks prior to granting access to any new hire. The background checks include the following:

- Social Security number trace
- Employment credit report
- Federal criminal checks
- Criminal county search
- Office of Foreign Assets Control (OFAC) check
- Multi-state instant criminal check with verification
- Nationwide Sex Offender Registry check

During the onboarding process, a checklist is completed for each employee. The New Hire Checklist ensures that all new hires complete the required activities, including receiving, reviewing, and acknowledging the appropriate forms and documents, such as Systems Usage Agreement, Confidentiality Agreement, and the Employee Handbook. The Employee Handbook addresses the employee conduct, ethics, information confidentiality, background and reference checks, and progressive discipline. The handbook is distributed to and acknowledged by personnel during orientation, and it is available for employees to review on the company's paycheck site.

In the event of termination, the Termination Checklist is used to track offboarding activities to ensure access is completely removed. Connectria immediately terminates the access rights of users when a resignation notice or notice of dismissal is received, and all badges, keys, laptops, and other pieces of equipment are collected.

Training

Connectria provides training programs for new and current employees to ensure they are aware of and able to perform their job responsibilities. Security training sessions cover security awareness, phishing, vishing, and incident response. Connectria uses the KnowBe4 training solution to provide security awareness training and training on other topics related to security and compliance.

Regulatory Requirements

Connectria adheres to relevant regulatory and legislative requirements that impact its operations and follows industry best practices and strict IT frameworks to ensure a high level of compliance. The organization uses the HIPAA, the Health Information Technology for Economic and Clinical Health Act (HITECH), the Payment Card Industry Data Security Standard (PCI DSS) Level 1, the Federal Information Security Management Act (FISMA), and National Institute of Standards and Technology (NIST) as relevant frameworks for compliance, and outside audits are completed for the following:

- SOC 1 & SOC 2 Type II
- HIPAA
- HITECH
- PCI DSS Level 1
- FISMA
- International Organization for Standardization (ISO) 27001
- Family Educational Rights and Privacy Act (FERPA)
- Bill 198
- General Data Protection Regulation (GDPR)
- HITRUST

Connectria has implemented controls to aid clients' compliance with the Ontario Securities Act (Bill 198). This Act:

- Broadens Ontario Securities Commission (OSC) powers
- Defines penalties for non-compliance and fraud
- Provides authority for regulators to develop rules to enhance investor confidence

The Canadian Securities Administrators issued three rules, under the authority granted by Bill 198:

- Multilateral Instrument 52-109: Improving the quality and reliability of reporting disclosure
- Multilateral Instrument 52-110: Strengthening the independence and authority of audit committees
- National Instrument 52-108: Improving public confidence in the integrity of financial reporting of public companies

RISK ASSESSMENT

Connectria has policies and procedures in place for conducting an annual risk assessment. A Risk Assessment Policy has been implemented to ensure that risks are managed appropriately, and a Risk Assessment Process has been documented to ensure that risk assessments are conducted properly and consistently. Per Connectria's Risk Assessment Policy, Connectria directors review all risks on the risk matrix at least quarterly. Risks are reviewed for likelihood and impact as well as updates on the risk. The Risk Assessment Process includes the following steps for conducting a risk assessment:

- Identify the scope of the risk analysis.
  - Review the completed Business Impact Analysis.
- Identify and document potential threats and vulnerabilities.
  - Consider the technology in use.
  - Look at web server configurations.
  - Is the technology publicly accessible?
- Assess the current security measures for the following:
  - Firewall
  - Access Control List
  - Port access restrictions
  - Two-factor authentication
- Determine the likelihood of threat occurrence.
- Determine the potential impact of threat occurrence.
- Determine the level of risk.
  - Complete the risk assessment matrix and rank the risk without mitigation controls.
- Identify additional mitigating security measures that may be implemented or purchased.
  - List all mitigating controls in place as well as additional mitigating controls needed.
  - Identify additional mitigating security measures that may be implemented or purchased.
- Update privacy, security, and risk assessment processes based on experiences with security incidents, changes in the environment or organization, and changes in prevention, detection, or response methods for security.
- Resolve risks using one of the following techniques:
  - Avoidance – Eliminates the risk by avoiding the activity that provides the risk.
  - Reduction – Reduce risks through controls that can reduce the likelihood or impact of a risk.
  - Transference – Reduce risks through shifting it to an outside entity.
  - Acceptance – Accept the risk, and when acceptance is selected, management acceptance must be documented.

In addition, the Risk Assessment Policy and Risk Assessment Procedure address requirements for developing and completing corrective action plans (CAPs). CAPs are conducted to ensure that the remedial security actions necessary to mitigate risks to operations, assets, individuals, and other organizations are documented. Connectria reviews CAPs for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions. CAPs are updated monthly based on the findings from security assessments, security impact analyses, and continuous monitoring activities.

MONITORING

Connectria conducts regular maintenance activities to ensure that the company remains secure and operational. The organization completes lists of daily tasks provided by the Security Operations Center (SOC) and the Network Operations Center (NOC). The task lists are separated by shift (first, second, and third), created at the end of each shift to detail completion of tasks and any relevant results, appropriate to the position, and relevant to the security goals of the organization. The organization's Maintenance Policy addresses procedures for conducting monitoring and diagnostic activities, including the following:

- Routine Maintenance – Tasks that are scheduled on a regular basis
- Break/Fix Maintenance – The result of an error condition usually resolved by a patch or replacement of a component
- System Upgrades – The transition of a product from one version to another
- Emergency Maintenance – Events that result in a complete disruption in computing services or render a large portion of the platform unavailable

Connectria uses Confluence as the primary reporting tool, allowing upper management to monitor performance. The Self-Service Reports in Confluence contain statistics on self-audits, contract statuses, customer detail and satisfaction, and open ticket items.

Description of Computerized Information Systems

Connectria maintains formally documented network diagrams, pictured below, that illustrate the company architecture and accurately reflect the system inventory.

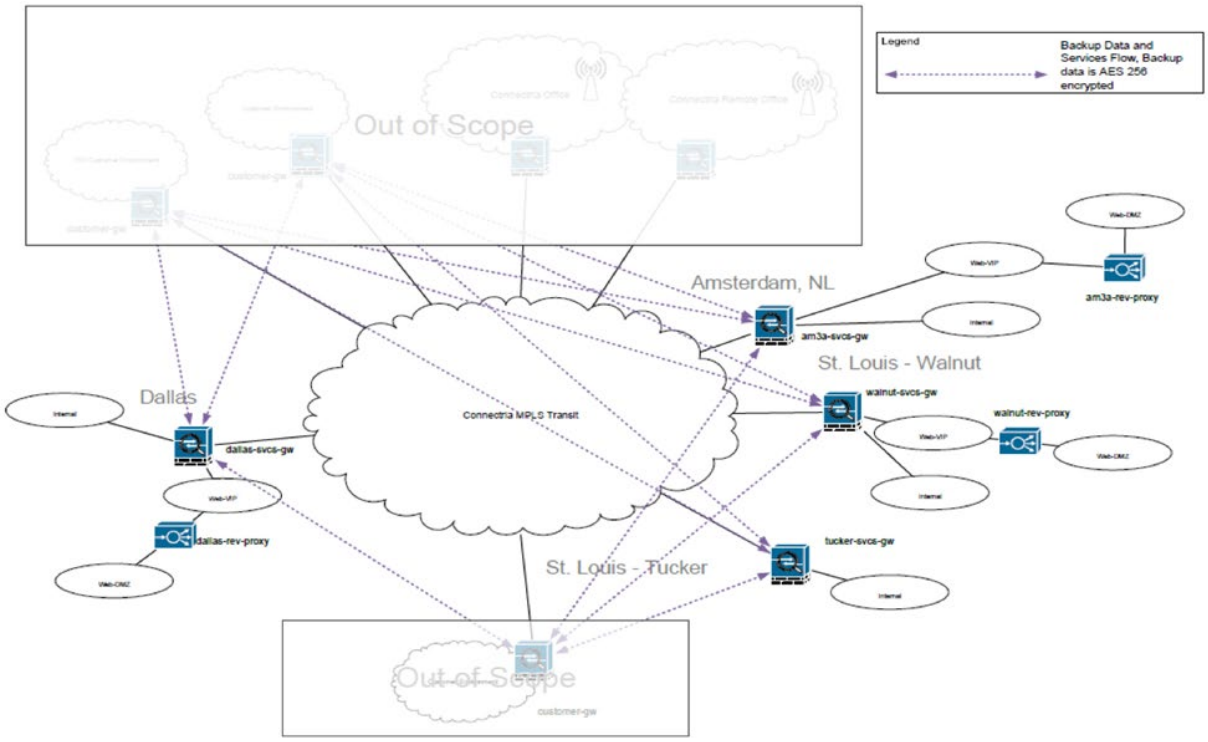


Figure 1: Topology Diagram of PCI Services Networks

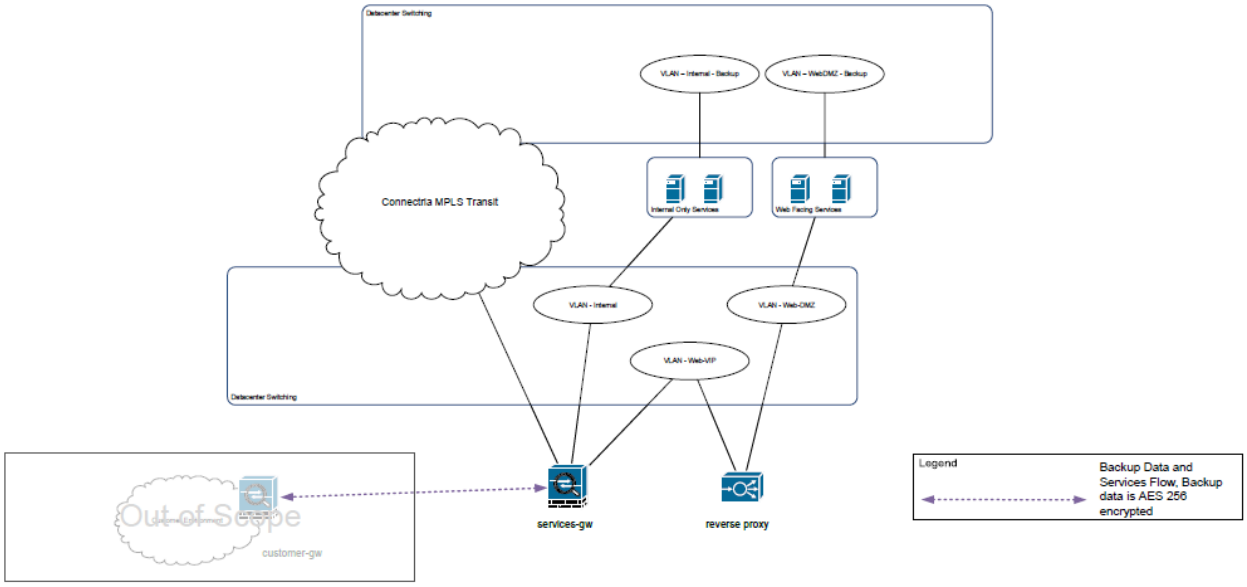


Figure 2: Site Local Topology for PCI Services Networks

The diagrams above include data centers and main offices, depict the logical isolation of sensitive systems and devices that may contain sensitive data, and demonstrate how data moves through the environment. Cisco ASA firewalls are used to segment the corporate network from the service provider network, and other systems are segmented from other networks in accordance with PCI DSS requirements. The Networking Team is responsible for maintaining the diagrams, including completing a biannual review and ensuring diagrams are updated following changes to the environment.

The organization also maintains an inventory of critical software. The software list is maintained by running an inventory scan on the devices and in accordance with the Software Approval Policy. Software scans are performed at least monthly, and the software inventory list includes a description of the function/use of each software application. The critical software in use includes the following:

- Active Directory
- Arbor
- Big Fix
- Citrix
- Commvault
- Confluence
- Duo Security Authentication Proxy 2.4.21
- IBM BigFix
- Infoblox
- Tripwire IP360
- Keypass
- Microsoft Office 365
- Nipper
- ProWatch
- QRadar
- RDM
- Remote Desktop Connection Manager
- Remote Desktop Manager
- SolarWinds
- Sophos
- Symantec Endpoint Protection
- Trend
- Tripwire Enterprise
- Veeam One
- Wasabi
- WatchGuard
- Wazuh
- Windows Azure Active Directory Sync
- Zerto

General IT Controls

Security Program

Connectria maintains documents that address security requirements, including the Security Program documentation. The security policies provide standards and procedures based on industry best practices and follow predominant IT security frameworks, including ISO 27001, HIPAA, PCI DSS, HITRUST, and NIST SP 800-53. The organization's security policies and Systems Usage Agreement outline the security responsibilities for all personnel. The Security Program contains a provision for disciplinary action and describes appropriate and inappropriate use depending on each topic covered. Documentation is stored in the organization's Confluence portal, which is protected using multi-factor authentication.

The organization maintains a Project Management Policy that defines how security is integrated to ensure that security risks are identified and addressed as part of each project, and

the following Project Management Institute (PMI) best practices are followed for project management:

- Identify stakeholders
- Plan communications
- Define requirements
- Create/develop the project team
- Plan risk management
- Define security requirements for project team, communications, implementation, and go live
- Verify deliverables

The organization maintains security policies and procedures for the transmission of sensitive information via electronic messages, including emails, text messages, instant messages, and voicemail messages. The Electronic Messaging Policy addresses the types of files blocked at the email gateway and the authentication methods that must comply with Connectria's Authentication Security Requirement. Only authorized personnel can access and make changes to electronic messaging applications.

A Systems Usage Agreement defines the acceptable use of Connectria's computing resources and communication systems. The agreement is used in conjunction with security training and the Employee Handbook to clearly communicate security requirements and responsibilities to all employees, who are required to sign the Systems Usage Agreement annually.

Connectria maintains a policy that addresses the requirements for moving, adding, and changing assets. The Asset Management Policy requires the following inventory items be maintained:

- Unique identifier and/or serial number
- Information system of which the component is a part
- Type of information system component (e.g., server, desktop, application)
- Manufacturer/model information
- Operating system type and version/service pack level
- Presence of virtual machines
- Application software version/license information
- Physical location (e.g., building/room number)
- Logical location (e.g., IP address, position with the IS architecture)
- Media access control (MAC) address
- Data ownership and custodian by position and role
- Operational status
- Primary and secondary administrators
- Primary user
- Mapped organizational communications and data flows

Incident Response

Connectria maintains an Incident Response Plan and Incident Response Procedures that address requirements for handling and responding to security incidents; a tabletop exercise

is conducted at least annually to test these procedures. Incident response generally consists of the following six stages:

1. Preparation
2. Identification
3. Assessment
4. Containment
5. Eradication
6. Follow-Up

All incidents, findings, and responses are required to be documented. A report is created three-to-five days after an incident is eradicated and may include the following:

- Technology configurations and other related factors that contributed to impact and downtime
- Gaps in processes and policies
- Circumvented processes or policies that contributed to the incident
- Past documented recommendations that could have mitigated the incident
- Opportunities for personnel training
- An improvement plan based upon the information collected in lessons learned, including:
    - Clear description of the action to be taken
    - Responsible party
    - Deadline for completion
    - Success stories (description of the successful, repeatable practices and procedures that took place)
    - Information that was needed sooner
    - Any additional tools or resources needed

Personnel involved in incident response obtain industry certifications to stay aware of the best practices for responding to security breaches. The technical certifications achieved are from recognized bodies, including AWS, ITIL, VMware, Microsoft, ISC2, Veeam, Red Hat, and various vendors. Certifications are tracked, including the expiration date, to ensure all staff maintain their certifications as appropriate.

The organization has a process in place that allows clients to report security breaches. Clients have direct access to Connectria's ticketing system to submit issues and track remediation.

Physical and Environmental Security

Physical access to Connectria's corporate office and systems is restricted to authorized personnel via physical security mechanisms. Onsite personnel are given photo keycard badges with role-based access. Biometrics as well as access badges are used to access secure areas, including servers and data centers. All power and telecommunications lines in the corporate office are terminated within a locked closet and travel underground into the building.

The organization maintains requirements for video surveillance cameras and live security. The Physical Security Policy requires access to every office, computer room, and work area

containing sensitive information to be physically restricted and monitored using video camera surveillance equipment, and CCTV cameras monitor all entrances to the building and data center space. The 365 Data Centers, the CyrusOne data center, the Equinix data center, and the Netrality Properties data centers are responsible for providing physical protections for Connectria data stored in their facilities. All data centers have live security personnel that alert emergency services as necessary, and each has cameras that feed to the NOC at the St. Louis corporate office.

The Visitor Policy defines how employees, contractors, vendors, and other individuals are authorized for access. Upon entrance to Connectria's facility, all visitors are required to sign a visitor log, which records each visitor's name, the date/time, the reason for the visit, and the visitor's agreement with policies. Visitor logs for the office location are virtually saved to a share. Visitors are given visitor badges at the corporate office, and all visitors at the data centers must present identification, wear badges, and be escorted at all times.

A Backup and Recovery Policy is in place that defines requirements for physically securing backup media. All backup media is encrypted following creation using AES 256-based keys. Backups are stored at data centers until being transferred to Iron Mountain for long-term storage.

Confluence and Iron Mountain are used to track media that is sent outside Connectria's facilities. Backups are stored at data centers until transferred to Iron Mountain for long-term storage. The Confluence portal is used to track location, owner, content, and sensitivity of all backup media. Iron Mountain is responsible for storing, logging, and tracking transports once it acquires media from Connectria.

The organization maintains an Asset Management Policy and a Data Destruction Policy that define the treatment, handling, disposal, destruction, and reuse of media. Per policy, all assets must be tracked from allocation through destruction via a unique identifier, to which are tied physical and logical locations, data owner/custodian, data type, and primary user. The organization sends equipment no longer in use to Iron Mountain for destruction. Media designated for destruction is stored in a locked box in a secured area within the data centers, and tapes and hard drives are degaussed before being sent to Iron Mountain, which provides a certificate of destruction for each item. All asset destruction follows Department of Defense guidance, and certificates are obtained for all destroyed media.

Logical Access

Connectria maintains a User Account Policy and a Service Account Policy that address requirements for assigning access to personnel. Access requests are tracked as tickets, and access rights and privileges are assigned to user IDs based on job role; accounts are requested by HR, approved by management, and granted access by Internal IT. Clients are registered and de-registered for online access to the organization's systems through procedures documented in the New User Setup Guide and Creating Customer Portal Users.

The organization uses Active Directory and Linux as its primary logical access control systems. Active Directory and Linux are used to enforce the separation of duties based on job

function, and all service accounts are maintained through Active Directory and governed by the Service Accounts Policy. Roles are tied to documented job descriptions within Active Directory, and access is assigned based on the principle of least privilege. The separation of duties is enforced using role-based access according to job descriptions and teams, and these roles and Active Directory groups are reviewed quarterly by the manager.

Windows and Linux complexity requirements are used to maintain the security and integrity of passwords. Password length and complexity requirements are controlled in Windows servers by global policy objects (GPO) and per-machine in Linux configurations. Connectria maintains a Password Policy that addresses password composition requirements, which are enforced in Linux and Active Directory. All passwords are required to have at least 10 characters composed of a combination of numeric, alphabetic, and special characters. The previous 24 passwords are remembered and cannot be reused. All Active Directory accounts lock out for 30 minutes following five failed login attempts, and the Linux accounts lock out for an hour following five failed login attempts. Windows machines and Linux accounts are configured to lock out after 15 minutes of inactivity. User password parameters require users to change passwords or passphrases at least once every 90 days.

Connectria has a process for assigning first-time passwords to new users. After a short training session, an Internal IT staff member changes the change password screen and forces the user to enter their new password. The Internal IT team member then verifies that the user with a new password can log in. If virtual is required, it is completed via virtual meeting with cameras enabled, and the IT personnel transfer control of their system to allow the user to type in their own password. Internal IT completes a similar process for resetting passwords for existing users.

The organization maintains a Remote Access Policy and a Multi-Factor Authentication Policy that define requirements for remote access technologies used in the company. The policies outline procedures for working remotely, and the use of approved two-factor authentication is defined. Authentication of remote users are implemented using a password or passphrase and at least one of the following methods:

- A cryptographic based technique
- Biometric techniques
- Hardware tokens
- Software tokens
- A challenge/response protocol
- Certificate agents

Connectria maintains a process for removing terminated or inactive accounts. The organization's Termination Policy requires access to be immediately revoked for any terminated/separated employees and requires account removal to be tracked via a ticket in the ticketing system. Access removal activities are dictated in the Termination Checklist, which requires collecting company-owned equipment and revoking access to systems. Additionally, reports are run monthly for accounts that have been inactive for 60 or more days, and tickets are created in response to the reports for disabling or removal of accounts.

Network Monitoring

Connectria maintains a Logging and Monitoring Policy that addresses the use of network logging and monitoring tools. QRadar is used for collecting logs on all systems, and the logs capture protocol type, timestamp, source and destination IP, and port information. Logs are all sent immediately to QRadar, which sends an active alert monitoring dashboard that is always monitored in the SOC. QRadar retains logs for at least one year, and the last three months' worth of logs are immediately available for analysis in QRadar.

The organization has implemented monitoring and intrusion-detection systems (IDS) to detect threats against systems that store, process, or transmit sensitive information. Connectria uses time synchronization technologies to synchronize all servers to Infoblox via Network Time Protocol (NTP). Antivirus, file-integrity monitoring (FIM), IDS, and security information and event management (SIEM) are always live-monitored by the SOC.

The organization uses the SolarWinds tool and generates reports to monitor system capacity and plan for future requirements. System capacity is discussed monthly at team meetings. The NOC uses tools, including SolarWinds, to monitor circuits, storage, and CPU utilization. In addition, customer availability reports are provided to the organization's customers on a monthly basis.

Configuration Management

Connectria maintains formally documented system configuration standards to ensure all systems and devices are configured appropriately and consistently. The Operating System Hardening Policy defines hardening standards for web, email, database, infrastructure management, and file servers. The configuration standards are based on industry best practices and IT security frameworks, including ISO 27001, HIPAA, PCI DSS, HITRUST, and NIST SP 800-53.

The organization updates configuration standards quarterly based on the results of vulnerability scans. The Security Team maintains the configuration standards, the Compliance Team scans new operating system configurations and changes, and the OS Team mitigates discovered vulnerabilities. The Compliance Team runs quarterly vulnerability scans, and configuration standards and hardened images are updated as appropriate, based on the scan results and corresponding tickets.

Personnel with system configuration responsibilities receive technical certifications to ensure that they remain aware of the appropriate ways to securely configure systems. Personnel receive certification from recognized bodies, including AWS, ITIL, VMware, Microsoft, ISC2, Veeam, Red Hat, and various vendors, and the list includes the name of the certification or educational degree obtained. Certifications are tracked, including the expiration date, to ensure all staff maintain their certifications as appropriate.

The organization maintains a Firewall Configuration Policy that requires quarterly review of firewall rules and justification for the rules that are configured. The Nipper Studio solution is used to facilitate the analysis of rule sets and to identify potential security issues, and tickets are created that list the Nipper scans performed and issues found.

Connectria maintains a Change Management Policy and Procedures document that defines how the organization manages technology-related changes to computing environments, including how changes are planned, communicated, evaluated, and implemented. The document defines roles and responsibilities for all personnel and requirements for testing, communicating, and evaluating the risk of changes.

The policy defines responsibilities for those involved in the change management process. Change Managers conduct Change Advisory Board (CAB) meetings, which must consist of at least two members of the Senior Management Team and at least three Change Managers. Change Advisors have technical expertise and provide technical guidance to the Change Manager, assisting in the assessment and prioritization of changes. The CAB is responsible for reviewing and analyzing change requests, coordinating changes, and reviewing outcomes. Change Management Sponsors are Connectria's Technology Managers and are responsible for ensuring requests meet change management policies, providing a timely approval decision, ensuring CAB members understand the change requested, initiating communications with Connectria and/or customers, and ensuring the availability of staff from impacted teams to successfully complete the change request.

All information technology employees and approved users have the capability to request changes. Change Requestors work with the Change Implementer to ensure all information is complete and accurate, communicate the change to the CAB within four hours of the CAB meeting, and attend the CAB meeting to represent the change. Change Requestors are responsible for drafting a notice that can be sent internally and/or to customers, if necessary, and for coordinating people from other teams that are necessary for the change and the validations. Change Requestors also identify the change as one of the following classifications:

- Standard change – A low-risk and low-impact change that is pre-defined and pre-approved. Standard changes are periodical changes that allow a standard operating procedure and are not required to go through the change management process.
- Minor change – A non-trivial change that has a low impact and low risk and undergoes the change management process, including CAB approval.
- Major change – A high-risk and high-impact change that could interrupt production environments and is required to go through change management, including CAB approval.
- Emergency change – A change that must be introduced as soon as possible due to likely negative service impacts. The change assessment may involve fewer steps due to the urgent nature of the issue; however, any emergency change must still be authorized through the change management approval process and may be reviewed by the CAB retroactively.

Change Implementers are assigned to coordinate and/or complete a specific change request. Change Implementers start the change request from the requestor and review it to ensure that all the steps are in the change request. They update the request, document the result including implementation start and stop times, and note any issues or previously unknown factors associated with the change.

All changes are required to undergo testing prior to implementation to minimize the likelihood of the change negatively impacting the environment. The tests address usability, security, and effects on other systems, and any issues identified during testing are documented and tracked through resolution. Changes that cannot be tested prior to implementation must have a reason documented in the Testing Plan section of the request and must be validated in production after the implementation has occurred.

Changes must be communicated to appropriate personnel during the planning stages and during the CAB approval stage. All participants and/or affected business units must be aware of the change through normal project/activity communications prior to the change being presented for scheduling to the CAB. The change request must include a complete description in business terms of what is being changed, when the change will occur, how the change will be implemented/backed out if necessary, how the change will be verified, and the impact and risks associated with the change. The Change Requestor is responsible for scheduling the change. All changes must have a risk assessment, test plan, and back-out plan information included in the change request prior to Sponsor authorization. Implementers and Sponsors assess the impact and potential consequences and ensure that back-out plans are reasonable and adequate.

Vulnerability Management

Connectria maintains policies that address requirements for conducting vulnerability assessments and managing security risks. A vulnerability assessment is conducted monthly, and any issues found are communicated to the system owners via a ticket. Additionally, the organization conducts regular internal and external scans and remediates findings in a timely manner. Per the Network Methodology Testing Policy and the Vulnerability Scanning Procedure, internal network vulnerability scans are scheduled to run monthly and after any significant change in the network, quarterly external vulnerability scans are performed by a PCI-approved scanning vendor, and internal/external penetration tests are performed quarterly against Connectria's management network.

The organization maintains patch management policies and procedures that define the use of sources for remediating vulnerabilities. The Patch Management Policy and the Patching Procedures define requirements for identifying new security vulnerabilities, assigning vulnerabilities a risk ranking that includes identification of all "high risk" and "critical" vulnerabilities, and using reputable outside sources for security vulnerability information. The outside sources used by Connectria include Tripwire IP360, Tripwire Security Intelligence Hub, and IBM BigFix. The organization's Patching Procedures require critical patches to be installed within 30 days. Security patching is implemented on a monthly basis, requiring all critical security patches to be installed within 30 days and all important security patches to be installed within 90 days. Internal and external vulnerability scans are required after any significant changes to the environment.

Additionally, Connectria maintains an Antivirus/Malware Policy and Vulnerability Management Policy that requires antivirus solutions be automatically updated. Antivirus is

installed on all machines and Windows and Linux servers, and Trend, Sophos, and Symantec report non-compliant machines to the SOC.

Data Security

Connectria stores data, including personal health information (PHI) and personally identifiable information (PII), on behalf of its clients as part of its managed services system. This data is classified and handled in accordance with the Data Classification/Ownership Policy that follows HITRUST and PCI DSS requirements. All data is categorized in one of four sensitivity classifications with separate handling requirements defined by minimum security baselines: Secret, Confidential, Internal, and Public. All data protection servers are classified as confidential due to PHI, and all other in-scope data is classified as internal.

Connectria maintains an Encryption and Hashing Policy that addresses requirements for implementing encryption to ensure data remains protected. Encryption is implemented for all confidential data, including both electronic transmissions and physical electronic media, prior to being sent outside the environment. Per policy, all information must be rendered unusable, unreadable, or undecipherable. This is accomplished using AES 256 encryption for backups, a secure method for key storage and transfer, mandated use of Perfect Forward Secrecy (PFS), strong protocols and ciphers, and a secure hashing algorithm. The Cryptographic Key Management Policy addresses requirements for managing encryption keys. The policy acknowledges cryptographic keys as the most sensitive type of data, limits who can access and manage them, and establishes a limited lifespan for keys.

Backup and Restoration

Connectria maintains a Backup and Recovery Policy that defines the process for backing up and recovering data in the event of a disaster or system malfunction. Backups are taken daily and written to tapes, which Iron Mountain stores and retains. Incremental or differential backups are conducted daily, and full backups are completed weekly to separate media. Data Owners are responsible for ensuring the frequency of backup operations, and the Data Protection Team is responsible for implementing backup requirements and managing all media containing backup data. Connectria conducts media inventories at least annually, and automated tools are used to track backups and check for current backups. Connectria uses Wasabi for offsite backups.

Business Continuity and Disaster Recovery

Connectria has implemented plans to maintain or restore operations and ensure availability of information at the required level and in the required timescales following interruption to, or failure of, critical business processes. Connectria has two types of continuity plans that are continually updated by operations management. The Technology Services Recovery Plan covers computer operations, infrastructure segments, and all server-based applications, and the Business Resumption Plan addresses all other departments within Connectria and defines procedures in the case of problems, emergencies, or disasters, including loss of computer operations. The business continuity plans are reviewed, tested, and updated annually. Tabletop exercises are performed annually based on specific scenarios, and plans are updated with lessons learned as appropriate.

Vendor Management

Connectria maintains a Vendor Risk Assessment Policy, a Vendor Management Policy, and a Contract Management Policy that define vendor management procedures and the role of subject area managers in monitoring vendors and third parties. The Vendor Risk Assessment Policy defines due diligence procedures that are completed prior to engaging with service providers. Per policy, vendor risks are examined to consider the type of access the external party will have to the information and information asset(s); practices and procedures to deal with security incidents and potential damages; the terms and conditions for the continuation of external party access in the case of a security incident; and legal and regulatory requirements and other contractual obligations relevant to the external party. The risk analysis utilizes the Vendor Risk Rating Matrix to assign a vendor risk rating of low, medium, or high. All third parties must sign a non-disclosure agreement prior to sharing information to ensure they agree to protecting confidential information and restricting disclosure.

Managers are responsible for following vendor management policies to ensure that third parties are maintaining compliance and effectively carrying out contracts. Each manager is responsible for following the vendor management policies for vendor assessment and evaluating them for security risks and maintaining the contracts. Third parties are reviewed annually and when contracts are renewed.

SUBSERVICE ORGANIZATIONS

Connectria uses industry-recognized subservice organizations to achieve operating efficiency and to obtain specific expertise. Connectria performs ongoing monitoring to determine that potential issues are identified timely to maintain the effectiveness of internal control. The following evaluations are conducted:

- Reviewing and reconciling output reports
- Holding periodic discussions with the subservice organization
- Making regular site visits
- Testing controls at the subservice organization
- Reviewing independent audit reports
- Monitoring external communications

The following are the principal subservice organizations used by Connectria:

- CyrusOne – data center services
- 365 Data Centers – data center services
- Netrality Properties – data center services
- Equinix – data center services
- Iron Mountain – backup and tape storage
- Wasabi – offsite backups

USER CONTROL CONSIDERATIONS

Connectria, LLC's services are designed with the assumption that certain controls will be implemented by user organizations. In certain situations, the application of specific controls at the user organization is necessary to achieve control objectives included in this report. Connectria, LLC's management makes control recommendations to user organizations and provides the means to implement these controls in many instances. Connectria, LLC also provides best practice guidance to clients regarding control elements outside the sphere of Connectria, LLC responsibility.

This section describes additional controls that should be in operation at user organizations to complement the Connectria, LLC controls. User control recommendations include:

- User organizations should implement sound and consistent internal controls regarding general IT system access and system usage appropriateness for all internal user organization components associated with Connectria, LLC.

- User organizations should ensure timely removal of user accounts for any users who have been terminated and were previously involved in any material functions or activities associated with Connectria, LLC's services.

- Transactions for user organizations relating to Connectria, LLC's services should be appropriately authorized, secure, timely, and complete.

- For user organizations sending data to Connectria, LLC, data should be protected by appropriate methods to ensure confidentiality, privacy, integrity, availability, and non-repudiation.

- User organizations should implement controls requiring additional approval procedures for critical transactions relating to Connectria, LLC's services.

- User organizations should report to Connectria, LLC in a timely manner any material changes to their overall control environment that may adversely affect services being performed by Connectria, LLC.

- User organizations are responsible for notifying Connectria, LLC in a timely manner of any changes to personnel directly involved with services performed by Connectria, LLC. These personnel may be involved in financial, technical or ancillary administrative functions directly associated with services provided by Connectria, LLC.

- User organizations are responsible for adhering to the terms and conditions stated within their contracts with Connectria, LLC.

- User organizations are responsible for developing, and if necessary, implementing a business continuity and disaster recovery plan (BCDRP) that will aid in the continuation of services provided by Connectria, LLC.

The list of user organization control considerations presented above and those presented with certain specified control objectives do not represent a comprehensive set of all the controls that should be employed by user organizations. Other controls may be required at user organizations. Therefore, each client's system of internal controls must be evaluated in conjunction with the internal control structure described in this report.

SECTION IV:
CONTROL OBJECTIVES AND RELATED CONTROLS

TEST METHODOLOGY

Section IV outlines the controls in place by Connectria, LLC and describes the tests of their effectiveness performed by the independent service auditor. The following methodologies were used in testing the suitability of the design and operating effectiveness of Connectria, LLC's controls:

Test Methodology	Description
Interview	The auditor inquired of relevant personnel to corroborate control placement or activity.
Review	The auditor obtained and read relevant Connectria, LLC documentation.
Observation	The auditor directly witnessed control placement or activity or evidence thereof.

The tables on the following pages outline the control objectives, controls in place, and independent testing relevant to the independent assessment of Connectria, LLC's control environment throughout the period October 1, 2019, to September 30, 2020.

Control Objective 1 – Organization and Administration			
Control Objective 1: Controls provide reasonable assurance that management provides oversight, segregates duties, and guides consistent implementation of security practices.			
Ctrl #	Controls Specified by Company	Testing Performed by Service Auditor	Test Results
1.1	The organization has appointed a Board of Directors that provides general oversight and leadership.	Reviewed Connectria's Limited Liability Company Agreement and verified the members act through meetings and written consents, and each member is entitled to vote based on their percentage ownership of the voting units Interviewed the Compliance Manager and determined Connectria is a Limited Liability Company (LLC), with board members consisting of holding companies Observed the members of holding companies consist of the following: • Bregal Sagemount II-B, L.P. • Chance Holdings, Inc. • Connectria Employee Holdings, LLC	No Relevant Exceptions Noted
1.2	The organization undergoes a series of audits and regulatory exams annually.	Interviewed the Compliance Analyst and determined Connectria's independent audits have been performed by KirkpatrickPrice Observed recent assessments performed by KirkpatrickPrice and determined the types of audits performed annually include the following: • HITRUST CSF v9.1 (dated April 30, 2020) • GDPR Compliance Audit Report (dated September 30, 2019) • PCI Report on Compliance (dated October 9, 2019) • Ontario Securities Act Compliance (Bill 198) (dated December 2, 2019) • FERPA (dated September 30, 2019) • FISMA Compliance Audit Report (dated September 30, 2019) • ISO/IEC 27001:2013 Compliance (dated September 30, 2019) • HIPAA (dated September 30, 2019) • SOC 2 Type II (dated November 26, 2019)	No Relevant Exceptions Noted

		• SOC 1 Type II (dated November 26, 2019) Observed audits contain recommendations if applicable and compared audits year-to-year and verified recommendations are acted upon as appropriate	
1.3	The organization obtains and reviews daily reports to monitor operational quality and control.	Reviewed the 2020 Self-Service Reports and verified it contains statistics on self-audits, contract statuses, customer detail and satisfaction, and open ticket items Interviewed the Compliance Analyst regarding the use of employee status reporting, surveys, and processes that include checks and balances and determined Confluence is also used as a reporting tool, which allows upper management to monitor performance and ensure appropriate quality controls are in place Observed during virtual onsite evidence of reports listed in the 2020 Operations Reports available in Confluence	No Relevant Exceptions Noted
1.4	The organization maintains a formally documented network diagram that illustrates the company architecture.	Reviewed the Network Diagram (dated January 7, 2020) and verified it includes a revision history table and description of recent changes, and it reflects the system inventory and the current network architecture and security design Interviewed the Compliance Analyst and determined the Networking Team is responsible for maintaining network diagrams and ensuring they are kept up to date as changes are made to the environment Observed Cisco ASA firewalls are used to segment the corporate network from the service provider network and other systems (e.g. wireless networks) are segmented from other networks in accordance with PCI DSS requirements Observed manage tickets and verified the biannual review of the network diagram	No Relevant Exceptions Noted
1.5	The organization maintains an inventory of critical systems.	Interviewed the Compliance Analyst and determined the system inventory is updated automatically using a portal solution	No Relevant Exceptions Noted

		whenever a new device with an in-scope IP is created Observed the system inventory and verified it includes the device name, device type, vendor, function, OS, and location, and the inventory matches network diagrams and agrees with devices found on vulnerability test results	
1.6	The organization maintains an inventory of critical software.	Interviewed the Compliance Analyst and determined the software list is maintained by running an inventory scan on the devices as well as following the Software Approval Policy Observed the software system inventory and verified the software list is maintained by running an inventory scan on the devices, software scans are performed at least monthly, and software inventory list includes a description of function/use of each	No Relevant Exceptions Noted
1.7	The organization conducts regular internal and external scans and remediates findings in a timely manner.	Reviewed the Network Methodology Testing Policy (dated February 26, 2020) and the Vulnerability Scanning Procedure (dated April 10, 2020) and verified internal network vulnerability scans are scheduled to run monthly and after any significant change in the network, quarterly external vulnerability scans are performed by a PCI-approved scanning vendor, and internal/external penetration tests are performed quarterly against Connectria's management network Interviewed the Compliance Analyst regarding the types of vulnerability scans performed and determined the frequency of scans and how remediation of issues found are documented and tracked Observed quarterly tests provided by an approved scanning vendor (ControlScan) and verified all scans resulted in passing CVSS scores Observed results of two recent internal vulnerability scans (October 30, 2019 and January 29, 2020) and verified issues were	No Relevant Exceptions Noted

		documented in vulnerability tickets and remediation tracked through resolution Observed results of the most recent internal/external penetration test (Q1 2020) and verified that certain high-risk issues were remediated and a rescan performed	
1.8	The organization has firewall configurations in place that enforce the segmentation of business networks.	Reviewed the Network Segmentation Policy (dated April 17, 2020) and verified it defines the separation of networks, each protected by a defined security perimeter Reviewed the Network Diagram (dated January 7, 2020) and verified the separation of the network environments, the use of Cisco ASA firewalls are used to segment the corporate network from the service provider network, and other systems are segmented from other networks in accordance with PCI DSS requirements Interviewed the Compliance Analyst regarding the use of firewalls to provide segmentation and determined quarterly penetration tests are performed to ensure there is no communication between the corporate and management networks	No Relevant Exceptions Noted
1.9	The organization's contractual agreements and company website communicate the scope of services provided to its clients.	Reviewed the Mutual NDA (dated October 1, 2019), the Master Services Agreement (dated March 12, 2020), the Statement of Work, and the Business Associate Agreement and verified that Connectria, LLC is a data center facility and managed services provider Interviewed the Compliance Analyst and determined the services offered to its customers are documented and in place Observed corporate website and verified it reflects the same information obtained via interview	No Relevant Exceptions Noted
1.10	The company maintains an organization chart that illustrates the company's traditional structure.	Reviewed the Executive Organization Chart (dated September 3, 2020) and a traditional chief-led hierarchical structure separated into departments that are predominantly led by directors	No Relevant Exceptions Noted

1.11	Management regularly communicates with personnel and enforces the use of the Employee Handbook and training to set the tone and direction for the company.	Interviewed the Compliance Analyst and determined upper management communication is primarily via email Observed evidence of newsletter distribution, monthly trainings, an Employee Handbook, and an internal Confluence page used to communication policy and procedure to all employees Observed annual formal security awareness training coupled with an ongoing approach to supplemental security trainings Observed tone and nature of the Employee Handbook and Code of Conduct documentation Observed policy documentation is available on the organization's Confluence page at all times for employees	No Relevant Exceptions Noted
1.12	The organization has a process in place for creating, approving, and updating policies and documentation.	Reviewed the Security Program (dated March 3, 2020) and verified the policy is reviewed and revised, if necessary, on an annual basis Interviewed the Compliance Manager and the Compliance Analyst and determined the security policies are reviewed at least annually, and old policies are retained indefinitely for reference Observed calendar evidence of meetings to update/review policies and verified the availability of historical policies on shared drives	No Relevant Exceptions Noted
1.13	The Employee Handbook and document agreements address the Code of Conduct and standards for ethical behavior.	Reviewed the Employee Handbook (dated July 1, 2020) and distributed news updates and verified that these documents are used to communicate the Code of Conduct, integrity, and ethics to new and current employees Interviewed the Compliance Analyst and determined that the Code of Conduct is communicated via the Employee Handbook, which all new employees sign, the Systems Usage Agreement, and Confidentially Agreement during orientation and annually;	No Relevant Exceptions Noted

		the Employee Handbook is available through all employees' Paycheck site for review; and regular communication via Connectria's internal intranet/blog site is used to communicate HR changes or updates	
1.14	Personnel complete daily task lists provided by the SOC and the NOC to ensure activities are completed relating to monitoring operational quality.	Reviewed NOC End of Shift Reports and the SOC Shift Task Lists and verified task lists are separated by shift (first, second, and third), created at the end of each shift to detail completion of tasks and any relevant results, appropriate to the position, and relevant to the security goals of the organization Interviewed the Compliance Manager and determined the lists of daily tasks are provided from the SOC and the NOC	No Relevant Exceptions Noted
1.15	The organization's Risk Assessment Policy and Risk Assessment Procedure addresses requirements for developing and completing corrective action plans (CAPs).	Reviewed the Risk Assessment Process (dated April 1, 2020) and Risk Assessment Policy (dated April 6, 2020) and verified it contains a section specifically referencing (CAPs) for the security program, a process for reviewing them, and a time-bound process for updating existing and open CAPs	No Relevant Exceptions Noted
1.16	The organization conducts an assessment on a quarterly basis to identify potential risks.	Reviewed the Risk Assessment Policy (dated April 6, 2020), Backup and Recovery Policy (dated March 31, 2020), and the Incident Response Procedures (dated February 28, 2020) and verified they address requirements for minimizing risks, and the policy is intended to be sufficient for multiple defined compliance frameworks Interviewed the Compliance Analyst and the Compliance Manager and determined the directors meet quarterly to review and update the risk matrix as needed Observed evidence of and results from quarterly reviews by directors of the risk assessment	No Relevant Exceptions Noted
1.17	The organization analyzes its risk assessment findings and business impact assessments to determine the controls to accept or mitigate risks.	Reviewed the Risk Assessment Process (dated April 1, 2020), the Risk Assessment Policy (dated April 6, 2020), and various business impact analyses created and updated by all departments and verified they detail impact and recovery methodology for	No Relevant Exceptions Noted

		all identified risks, and the risk matrix and Business Impact Analysis (BIA) address the choice to mitigate or accept risk Interviewed the Compliance Manager and determined directors meet quarterly to review risk analysis and the Compliance Team meets with business units annually to review BIA Observed evidence of quarterly meetings (emails and meetings) and verified they were conducted for reviewing the risk matrix sent to directors Observed completed risk assessments in the last nine months culminating in the updating of a thorough risk matrix identifying logical and physical risks to the environment	
Control Objective 1 Conclusion: Based on the tests of operating effectiveness, the controls described above provide reasonable assurance that management provides oversight, segregates duties, and guides consistent implementation of security practices.			

Control Objective 2 –Security Program			
Control Objective 2: Controls provide reasonable assurance that information security policies are maintained to set the security tone for the company and create security awareness.			
Ctrl #	Controls Specified by Company	Testing Performed by Service Auditor	Test Results
2.1	The organization has a Systems Usage Agreement that is used to communicate the use of systems and information to internal personnel.	Reviewed the Systems Usage Agreement (dated February 28, 2020) and verified the agreement defines appropriate and inappropriate use of Connectria's computing systems and related components Interviewed the Compliance Analyst and determined the organization's security policy/procedure documentation defines the requirements for proper use of the system, and all employees annually sign a Systems Usage Agreement that defines the acceptable use of Connectria's computing resources and communication systems Observed a sample of 4 of 39 new hire employee files and verified Systems Usage Agreements were signed during onboarding	No Relevant Exceptions Noted
2.2	The organization maintains a Project Management Policy that defines how security is integrated into each project.	Reviewed the Project Management Policy (dated April 6, 2020) and verified that the following Project Management Institute (PMI) best practices for project management are followed, which includes security requirements: • Stakeholders must be identified • Plan communications • Define requirements • Create/develop the project team • Plan risk management • Define security requirements for project team, communications, implementation and go live • Verify deliverables Interviewed the Compliance Manager and determined security is integrated into project management methods to ensure that security risks are identified and addressed as part of each project	No Relevant Exceptions Noted

		Observed 10 change tickets from the assessment period and verified the following topics are documented, as appropriate, to analyze security risks: • Business justification • Priority • Risk level • Identification of risks • Customer/business impact	
2.3	The organization maintains security policies and procedures for the transmission of sensitive information via electronic messages.	Reviewed the Electronic Messaging Policy (dated April 6, 2020) and verified the types of files blocked at the email gateway, authentication methods must comply with Connectria's Authentication Security Requirements, and access and changes to electronic messaging applications can only be done by authorized personnel Interviewed the Compliance Analyst and determined the use of all types of electronic messaging, such as emails, text messages, instant messages, and voicemail messages, to ensure the secure transmission of sensitive data Observed evidence of electronic messaging blocked at the email gateway	No Relevant Exceptions Noted
2.4	The organization maintains an information system security plan.	Reviewed the Security Program document (dated March 3, 2020) and verified the review and revision of security policies are required to be performed annually by the Compliance Team Interviewed the Compliance Analyst and determined security policies and all related documentation are reviewed annually, stored in Confluence, and accessible to all employees Observed the revision history section of the Security Program document and related security policies and verified policies are reviewed and changes logged as appropriate Observed the Confluence portal used by Connectria and verified policies are maintained and accessible to all employees	No Relevant Exceptions Noted

2.5	The organization's Maintenance Policy addresses procedures for conducting monitoring and diagnostic activities.	Reviewed the Maintenance Policy (dated April 9, 2020) and verified the following maintenance activities are conducted: • Routine Maintenance – Tasks that are scheduled on a regular basis • Break/Fix Maintenance – The result of an error condition usually resolved by a patch or replacement of a component • System Upgrades – The transition of a product from one version to another • Emergency Maintenance – Events that result in a complete disruption in computing services or render a large portion of the platform unavailable Interviewed the Compliance Analyst regarding the organization's procedures and determined maintenance of information systems and hardware is performed in accordance with the maintenance policy at supplier-recommended service intervals, and maintenance and the performance of updates is correlated to recovery objectives within the business continuity/disaster recovery plan Observed tickets associated with maintenance activities and evidence of review of reports used for maintenance activities by the NOC	No Relevant Exceptions Noted
2.6	The organization maintains documents that address requirements for its security requirements, including the Security Program documentation.	Reviewed the Security Program (dated March 3, 2020) and verified the review and revision of security policies are required to be performed annually by the Compliance Team Interviewed the Compliance Analyst and determined security policies and all related documentation are reviewed annually, stored in Confluence, and accessible to all employees Observed the revision history section of the Security Program document and related security policies and verified policies are reviewed and changes logged as appropriate	No Relevant Exceptions Noted

		Observed the Confluence portal used by Connectria and verified policies are maintained and accessible to all employees Observed the security policy documentation contains a provision for disciplinary action and describes appropriate and inappropriate use depending on each specific topic covered	
2.7	The Security Program addresses the organization's security requirements and procedures.	Reviewed the Security Program (dated March 3, 2020) and verified it contains a provision for disciplinary action and describes appropriate and inappropriate use depending on each specific topic covered Interviewed the Compliance Analyst and determined security policies and all related documentation are reviewed annually, stored in Confluence, and accessible to all employees; the security policies provide standards and procedures based on industry best practices and follow predominant IT security frameworks, including ISO 27001, HIPAA, PCI DSS, HITRUST, and NIST SP 800-53 Observed the revision history section of the Security Program document and related security policies and verified policies are reviewed and changes logged as appropriate Observed the Confluence portal used by Connectria and verified policies are maintained and accessible to all employees	No Relevant Exceptions Noted
2.8	The organization's security policies and agreements define the security responsibilities for all personnel.	Reviewed the Connectria Charter (dated April 12, 2019), the Security Program (dated March 3, 2020), and the Systems Usage Agreement (dated February 28, 2020) and verified they outline the security responsibilities for all personnel Interviewed the Compliance Manager and determined the organization's security policies and the ways security responsibilities are defined, acknowledged, and accepted by personnel	No Relevant Exceptions Noted
2.9	The organization conducts security awareness training with its employees.	Reviewed the Security Program (dated March 3, 2020) and verified the following	No Relevant Exceptions Noted

		responsibilities concerning the provisioning of training are defined: • Executive Management – Support training and awareness of all personnel to the security policies • Security and Compliance Group – Implement a process for ensuring that Connectria's plans for conducting security testing, training, and monitoring activities associated with organizational information systems are developed and maintained and are executed in a timely manner • Managers – Ensure that personnel receive the appropriate security training Interviewed the Compliance Analyst and determined the use of the KnowBe4 training solution to provide security awareness training and other topics related to security and compliance Observed training records for the assessment period and verified the following training and test results were documented for all employees: • Security Awareness Training • Phishing Training • Vishing Training • Incident Response Training	
2.10	The organization requires that all personnel acknowledge the Systems Usage Agreement to ensure that they are aware of their security responsibilities.	Interviewed the Compliance Analyst and determined internal users accept the Systems Usage Agreement at hire and on an annual basis; external users are not allowed data or systems access; and all employees are told at hire that the security policies are stored in Confluence Observed all employees are documented having accepted the Systems Usage Agreement at hire and on an annual basis Observed Systems Usage Agreement communicates proper use of systems and information and verified that employees are required to acknowledge the document	No Relevant Exceptions Noted

		Observed all security policies are available on the Confluence portal	
2.11	The organization maintains an Incident Response Plan and Incident Response Procedures that define how to handle and remediate security incidents.	Reviewed the Connectria Incident Response Plan (dated February 28, 2020) and the Incident Response Procedures (dated February 28, 2020) and verified that incident response procedures are designed to manage security-related incidents competently, efficiently, and legally, and the following six stages are defined for identifying, assessing, controlling, and eradicating an security-related incident: • Preparation • Identification • Assessment • Containment • Eradication • Follow-up Interviewed the Compliance Analyst regarding the organization's incident response procedures and the annual testing of such procedures	No Relevant Exceptions Noted
2.12	The organization stores all policies on the company intranet, and the policies are available for employees to review.	Interviewed the Compliance Analyst and determined and all employees are told at hire that the security policies are stored in Confluence Observed all security policies are available on the Confluence portal	No Relevant Exceptions Noted
2.13	The organization's incident response procedures are reviewed, tested, and updated at least annually.	Reviewed the Connectria Incident Response Plan (dated February 28, 2020) and the Incident Response Procedures (dated February 28, 2020) and verified incident response procedures are designed to manage security-related incidents competently, efficiently, and legally Interviewed the Compliance Analyst regarding the organization's incident response procedures and the annual testing of such procedures Observed results of a recent 2020 tabletop exercise and verified the procedures are discussed and tested annually, at a minimum	No Relevant Exceptions Noted

2.14	Personnel obtain industry certifications in order to stay aware of the best practices for responding to security breaches.	Reviewed the Certification List (dated April 22, 2020) and verified certifications are tracked, including the expiration date, to ensure all staff maintain their certifications as appropriate Interviewed the Compliance Manager regarding training attended by technical and security staff and determined certifications obtained by staff are logged for each individual with security breach responsibilities Observed the technical certifications list consists of certifications issued by recognized bodies, including AWS, ITIL, VMware, Microsoft, ISC2, Veeam, RedHat, and various vendors, and the list includes name of the certification or educational degree obtained	No Relevant Exceptions Noted
2.15	Clients use the organization's ticketing system to escalate potential incidents to appropriate personnel.	Reviewed the Connectria Master Services Agreement (dated March 13, 2020) and verified the support and contact information is supplied to clients Interviewed the Compliance Analyst regarding the ways clients and users inform the organization about security breaches and submit complaints and determined clients have direct access to Connectria's ticketing system to submit issues and track remediation Observed evidence of user-created tickets and response by NOC personnel as well as evidence of email correspondence with clients for various issues and verified clients have direct lines of communication with appropriate Connectria personnel to file complaints or report issues	No Relevant Exceptions Noted
2.16	The organization maintains policies that address the procedures for introducing new systems to the environment.	Reviewed the Change Management Policy (dated April 8, 2020), the Asset Management Policy (dated April 6, 2020), and the Software Approval Policy (dated April 6, 2020) and verified their appropriateness concerning the approval process for new systems	No Relevant Exceptions Noted

		Interviewed the Compliance Manager and determined Connectria's procedures for the Change Advisory Board (CAB) and the Sponsor to approve new systems	
2.17	Documentation is stored in the organization's Confluence portal, which is protected using multi-factor authentication.	Interviewed the Compliance Analyst and determined Confluence used to store system documentation and verified the system sits behind a web application firewall (WAF) and requires multi-factor authentication Reviewed the Multi-Factor Authentication Policy (dated April 6, 2020) and verified access requiring multi-factor authentication is defined Observed inventories and system documentation are available in Confluence Observed multi-factor authentication access is required to access Confluence	No Relevant Exceptions Noted
2.18	The organization has a process for defining how incidents and alerts are monitored.	Reviewed the Validation of the Incident section of the Connectria Incident Response Procedures (dated February 28, 2020) and verified monitoring activities are defined for intrusion detection/prevention, file-integrity monitoring, and detection of unauthorized wireless access points Interviewed the Compliance Manager and determined procedures to report, log, document, and remediate all types of security-related incidents Observed the Incident Management Reports – Compliance List (dated April 10, 2020) and verified the types of incident reports submitted relating to intrusion detection/prevention, file-integrity monitoring, and detection of unauthorized wireless access points	No Relevant Exceptions Noted
2.19	The security policies are reviewed and updated at least annually.	Reviewed the Security Program (dated March 3, 2020) and verified the review and revision of security policies are required to be performed annually by the Compliance Team Interviewed the Compliance Analyst and determined security policies and all related documentation are reviewed annually,	No Relevant Exceptions Noted

		stored in Confluence, and accessible to all employees Observed the revision history section of the Security Program document and related security policies and verified policies are reviewed and changes logged as appropriate Observed Confluence is used by Connectria and verified policies are maintained and accessible to all employees	
2.20	The organization maintains a policy that addresses the requirements for moving, adding, and changing assets.	Reviewed the Asset Management Policy (dated April 6, 2020) and verified it defines the following inventory items be maintained: • Unique identifier and/or serial number • Information system of which the component is a part • Type of information system component (e.g., server, desktop, application) • Manufacturer/model information • Operating system type and version/service pack level • Presence of virtual machines • Application software version/license information • Physical location (e.g., building/room number) • Logical location (e.g., IP address, position with the IS architecture) • Media access control (MAC) address • Data ownership and custodian by position and role • Operational status • Primary and secondary administrators • Primary user • Mapped organizational communications and data flows Interviewed the Compliance Analyst regarding the organization's asset management program and determined all in-scope assets are managed during moves, adds, and changes and are tracked in the ticketing system Observed during virtual onsite evidence of the asset tracking maintained in the	No Relevant Exceptions Noted

		Confluence portal and verified compliance with the Asset Management Policy	
2.21	The organization has daily operational security processes in place that relate to internal security.	Reviewed the SOC Shift Task List and three SOC End of Shift reports and verified task lists are broken down by shift (first, second, and third), and the end of shift lists are created at the end of every shift detailing completion of tasks and any relevant results of the tasks Interviewed the Compliance Analyst regarding daily tasks performed by SOC staff and determined each shift certain defined tasks need to be accomplished in addition to normal monitoring	No Relevant Exceptions Noted
2.22	The policies are maintained that define the use of all critical technologies used in the organization.	Reviewed the following documentation and verified appropriate use is defined in the appropriate policy, depending on the technology • Data Classification/Ownership Policy (dated April 6, 2020) • Remote Access Policy (dated April 6, 2020) • Asset Management Policy (dated April 6, 2020) • Access Control Policy (dated February 28, 2020) • Systems Usage Agreement (dated February 28, 2020) • Security Program (dated March 3, 2020) Interviewed the Compliance Manager and determined the critical technologies used by Connectria and policies that define their appropriate use Observed critical technologies in use include the following: • Active Directory • Citrix • Commvault • Duo Security • Microsoft Office 365 • QRadar • SolarWinds • Sophos Antivirus • Tripwire	No Relevant Exceptions Noted

		• Veeam • Confluence • Trend Antivirus • IBM BigFix	
2.23	The organization enforces requirements for the segregation of duties and assigning role-based access to systems.	Interviewed the Compliance Analyst and the Director of Internal IT regarding authorization and implementation of user IDs and determined access requests are tracked as tickets, accounts are approved by management, and access is granted by Internal IT Observed evidence of account creation tickets, 2019 fourth quarter employee access reviews, and 2020 first quarter employee access reviews and verified that administrative rights are limited to Internal IT staff	No Relevant Exceptions Noted
2.24	The organization maintains a Remote Access Policy that defines requirements for remote access technologies used in the company, including the use of multi-factor authentication.	Reviewed the Remote Access Policy (dated April 6, 2020) and the Multi-Factor Authentication Policy (dated April 6, 2020) and verified procedures for working remotely and the use of approved two-factor authentication are defined Interviewed the Compliance Analyst and determined Connectria's use of Duo for multi-factor authentication, and Connectria utilizes a smartphone application and physical tokens Observed via virtual onsite the use of the Duo technology and verified multi-factor authentication is enforced for remote access by all devices	No Relevant Exceptions Noted
Control Objective 2 Conclusion: Based on the tests of operating effectiveness, the controls described above provide reasonable assurance that information security policies are maintained to set the security tone for the company and create security awareness.			

Control Objective 3 – Human Resources			
Control Objective 3: Controls provide reasonable assurance that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered. Controls ensure the reduction in risk of theft, fraud, and misuse of facilities.			
Ctrl #	Controls Specified by Company	Testing Performed by Service Auditor	Test Results
3.1	The organization maintains an Employee Handbook that is distributed to and acknowledged by all personnel.	Reviewed Connectria's Employee Handbook (dated July 1, 2020) and verified that it includes the Code of Conduct, statement on ethics, information confidentiality, background and reference checks, and progressive discipline, and the handbook contains an employee acknowledgement, in which the employee agrees to receipt of, understanding of, and compliance with the handbook Interviewed the Manager of Human Resources and determined the handbook is distributed to all new hires at new employee orientation and the handbook is available to all employees on the paycheck site Observed a sample of 4 of 39 new employee records and verified they read and acknowledged the Employee Handbook	No Relevant Exceptions Noted
3.2	The organization maintains job descriptions for critical positions that define job responsibilities.	Reviewed a representative sample of job descriptions and verified they address primary roles and responsibilities, qualifications and education requirements, and preferred skills Interviewed the Compliance Analyst and determined the formal job descriptions define roles and responsibilities for key positions within the organization	No Relevant Exceptions Noted
3.3	The organization maintains onboarding and offboarding checklists and policies for hiring and terminating employees and contractors.	Reviewed the Onboarding Policy (dated March 19, 2020) and the Termination Policy (dated April 6, 2020) and verified hiring and termination procedures are outlined and documented Interviewed the Compliance Analyst and determined potential hires are tested and undergo multiple interviews; HR follows a checklist for onboarding of new hires; a	No Relevant Exceptions Noted

		termination checklist is used by HR to ensure all badges, keys, laptop, and other pieces of equipment are collected; and Connectria immediately terminates the access rights of users when a resignation notice or notice of dismissal is received Observed a representative sample of completed new hire checklists (4 of 39) and termination checklists (3 of 29) and verified onboarding and termination procedures were followed during the assessment period	
3.4	The organization distributes the appropriate forms and documents to personnel during onboarding.	Interviewed the Compliance Analyst and determined new hires must acknowledge various documents and agreements, including Employee Handbook, Systems Usage Agreement, and Confidentiality Agreement, and HR follows a New Hire Checklist to ensure all steps in the onboarding process are met Observed a representative sample of 3 of 49 completed New Hire Checklists and verified I-9 form and background check authorization for each new hire	No Relevant Exceptions Noted
3.5	The organization conducts background checks on all potential hires.	Reviewed the Onboarding Policy (dated March 19, 2020) and verified that it defines the background check requirements Interviewed the Compliance Analyst regarding procedures followed by HR to conduct a criminal and financial background check prior to granting access to any new hire Observed that background checks are performed by Sterling Talent Solutions Observed completed background checks for a sample of employees (3 of 29) hired during the assessment period and verified the following checks were performed: • SSN trace • Employment credit report • Federal criminal checks • Criminal county search • OFAC check • Multi-state instant criminal check with verification	No Relevant Exceptions Noted

		• Nationwide Sex Offender Registry check	
3.6	The organization adheres to regulatory measures that impact its operations.	Reviewed the Security Program (dated March 3, 2020) and verified configuration standards are based on NIST special publications, PCI DSS requirements, and other security frameworks Interviewed the Compliance Analyst regarding policy/procedures followed to ensure system configuration standards are documented and maintained and determined system configuration policies are reviewed annually at a minimum, and follow industry best practices and IT security frameworks, including ISO 27001, HIPAA, PCI DSS, HITRUST, and NIST SP 800-53	No Relevant Exceptions Noted
Control Objective 3 Conclusion: Based on the tests of operating effectiveness, the controls described above provide reasonable assurance that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered. Controls ensure the reduction in risk of theft, fraud, and misuse of facilities.			

Control Objective 4 – Environmental Security			
Control Objective 4: Controls provide reasonable assurance that physical assets are adequately protected against environmental hazards and related damage.			
Ctrl #	Controls Specified by Company	Testing Performed by Service Auditor	Test Results
4.1	Data centers have protections in place that guard against external and environmental hazards.	Interviewed the Compliance Analyst and determined that environmental security is the responsibility of the data centers Observed that the organization obtained third-party assessment reports from the following vendors to evaluate vendor compliance: • Netrality Properties • CyrusOne, LLC • 365 Data Centers • Equinix	No Relevant Exceptions Noted
Control Objective 4 Conclusion: Based on the tests of operating effectiveness, the controls described above provide reasonable assurance that physical assets are adequately protected against environmental hazards and related damage.			

Control Objective 5 – Physical Security

Control Objective 5: Controls provide reasonable assurance that physical access to critical applications and data is limited to authorized individuals.

Ctrl #	Controls Specified by Company	Testing Performed by Service Auditor	Test Results
5.1	The organization maintains a Physical Security Policy that defines the use of physical safeguards in the facilities.	Reviewed the Physical Security Policy (dated March 19, 2020) and verified the policy mandates updating, contains visitor policies, facility security, and logging/retention policies	No Relevant Exceptions Noted
5.2	The organization secures its telecommunication cables underground to ensure the data they are carrying is not intercepted or damaged.	Interviewed the Compliance Analyst and determined that all power and telecommunications lines in the corporate office are terminated within a locked closet and travel underground into the building Observed via a virtual walkthrough that all power and telecommunications lines in the corporate office are terminated within a locked closet and travel underground into the building via cameras	No Relevant Exceptions Noted
5.3	All assets are managed in Confluence, and the types of data an asset manages defines whether or not an asset can connect to the network.	Reviewed the Asset Management Policy (dated April 6, 2020) and verified requirements for the asset management program are documented Interviewed the Compliance Analyst and determined all assets are tracked in the portal, and the type of data clarifies what networks to which assets may be attached Observed evidence of asset tracking in the Confluence portal including nature of data, owner, date, and source	No Relevant Exceptions Noted
5.4	The organization has physical security measures in place to ensure that unauthorized personnel cannot access secure areas.	Reviewed the Physical Security Policy (dated March 19, 2020) and verified it addresses facility security Interviewed the Compliance Analyst and determined the use of biometric and badge access at all sites Observed via a camera review and virtual walkthrough and verified physical security mechanisms, including biometrics and badge access, are in place	No Relevant Exceptions Noted

5.5	The organization maintains an Asset Management Policy and a Data Destruction Policy that define the treatment, handling, disposal, destruction, and reuse of media.	Reviewed the Data Destruction Policy (dated April 6, 2020) and the Asset Management Policy (dated April 6, 2020) and verified that all assets must be tracked from allocation through destruction via a unique identifier, to which are tied physical and logical locations, data owner/custodian, data type, and primary user Interviewed the Compliance Analyst and determined asset destruction follows Department of Defense guidance and certificates are obtained for all destroyed media Observed tickets and verified data media sanitization for a subset of reused media Observed certificates verifying destruction of media at the end of its life	No Relevant Exceptions Noted
5.6	Backup media is stored and protected at Iron Mountain.	Interviewed the Compliance Analyst and determined backups are stored at data centers until transferring to Iron Mountain for long-term storage Observed portal is used to track location, owner, content, and sensitivity of all backup media, and backup media is encrypted on creation using AES 256-based keys Observed that the organization obtained a SOC 2 and PCI AOC for Iron Mountain	No Relevant Exceptions Noted
5.7	The organization visits and reviews the offsite facility at least once annually.	Reviewed the Backup and Recovery Policy (dated March 31, 2020) and verified the offsite facility must be visited at least annually Interviewed the Compliance Analyst and determined the offsite facility is visited annually by employees to validate security and environmental protections	No Relevant Exceptions Noted
5.8	Confluence and Iron Mountain are used to track media that is sent outside Connectria's facilities.	Interviewed the Compliance Analyst and determined backups are stored at data centers until transferred to Iron Mountain for long-term storage Observed the Confluence portal is used to track location, owner, content, and sensitivity of all backup media and verified	No Relevant Exceptions Noted

		transports by Iron Mountain are logged and tracked by Iron Mountain	
5.9	The organization sends equipment no longer in use to Iron Mountain for destruction.	Reviewed the Data Destruction Policy (dated April 6, 2020) and verified destruction procedures are documented Interviewed the Compliance Analyst and determined tapes and hard drives are degaussed before being sent to Iron Mountain for destruction, who provides a certificate of destruction for each item Observed a Certificate of Data Destruction from Iron Mountain and verified the organization obtains evidence of data destruction	No Relevant Exceptions Noted
5.10	Media designated for destruction is securely stored in data centers prior to disposal.	Interviewed the Compliance Analyst and determined media designated for destruction is stored in a locked box in a secured area within the data centers prior to being handed over to Iron Mountain for destruction Observed documentation evidence of tracking and destruction of media	No Relevant Exceptions Noted
5.11	The organization maintains service contracts with significant vendors.	Interviewed the Compliance Analyst and determined service contracts are maintained with significant vendors Observed a sample of a Service Provider Agreements with Predatar and Equinix as well as samples of maintenance contracts from other vendors provided by Infrastructure Team	No Relevant Exceptions Noted
5.12	The organization is equipped with video cameras and live security personnel for monitoring the corporate office and data centers.	Reviewed the Physical Security Policy (dated March 19, 2020) and verified the policy requires access to every office, computer room, and work area that contains sensitive information be physically restricted and monitored using video camera surveillance equipment, and CCTV cameras monitoring all entrances to the building and data center space Interviewed the Compliance Manager and determined each data center has live security personnel who alert emergency services as necessary, and each data center	No Relevant Exceptions Noted

		has cameras which always feed to the NOC at the St. Louis office Observed camera screenshots and verified placement and that cameras are being monitored virtually by NOC personnel	
5.14	The organization maintains documented policies that define procedures for assigning badges to personnel and visitors in the corporate office and data centers.	Reviewed the Visitor Policy (dated March 19, 2020) and the Physical Security Policy (dated March 19, 2020) and verified visitor procedures are documented and visitor badges must be worn while in the data center Interviewed the Compliance Analyst and determined employees wear employee badges at all times, visitors are given visitor badges at the corporate office, and all visitors at the data center must wear badges and present ID and escorted at all times Observed all employees are currently home-based due to COVID-19 and visitors are not being allowed into the office	No Relevant Exceptions Noted
5.15	The organization uses visitor logs at its corporate office and data centers to track visitor access.	Reviewed the Logging and Monitoring Policy (dated April 6, 2020) and the Visitor Policy (dated March 19, 2020) and verified the organization has procedures for registering visitors Interviewed the Compliance Analyst and the Compliance Manager and determined logs are used and maintained at all data centers Observed visitor logs from company headquarters facility and verified logs contained all required information; visitor logs for the office location are saved virtually; and visitor logs contain name, date/time, reason for visit, and agreement with policies	No Relevant Exceptions Noted
Control Objective 5 Conclusion: Based on the tests of operating effectiveness, the controls described above provide reasonable assurance that physical access to critical applications and data is limited to authorized individuals.			

Control Objective 6 – Logical Access			
Control Objective 6: Controls provide reasonable assurance that logical access to programs, data, and operating systems is restricted to authorized personnel.			
Ctrl #	Controls Specified by Company	Testing Performed by Service Auditor	Test Results
6.1	The organization uses Active Directory to restrict access to utility programs that might be capable of overriding the system.	Reviewed the Service Accounts Policy (dated April 6, 2020) and the User Account Policy (dated April 6, 2020) and verified it addresses access requirements for personnel Interviewed the Compliance Analyst and determined all service accounts are maintained through Active Directory, governed by the Service Accounts Policy, and limited in access to only access required for functionality Observed Active Directory service accounts are documented, limited in access, and reviewed frequently Observed Linux utility accounts shells are directed to an non-login	No Relevant Exceptions Noted
6.2	Active Directory and Linux are used to enforce the separation of duties based on job function.	Reviewed job descriptions for personnel and verified that that they address job responsibilities Interviewed the Compliance Analyst and determined the separation of duties is enforced using a role-based access based on job descriptions and teams, and these roles and Active Directory groups are reviewed quarterly by the manager Observed evidence of Active Directory and Linux access being granted and verified a manager must approve access	No Relevant Exceptions Noted
6.3	Internal IT assigns access rights and privileges to user IDs based on job role.	Reviewed the Access Control Policy (dated February 28, 2020), the Elevated Account Policy (dated February 26, 2020), the Password Policy (dated April 6, 2020), the Service Accounts Policy (dated April 6, 2020), and the User Account Policy (dated April 6, 2020) and verified the process for authorizing and implementing user IDs are	No Relevant Exceptions Noted

		documented and requires that access be assigned based on role Interviewed the Compliance Analyst and the Director of Internal IT and determined access requests are tracked as tickets, accounts are approved by management, and access is granted by Internal IT Observed evidence of account creation tickets and verified management approval in account request tickets and administrative rights are limited to Internal IT staff	
6.4	The organization uses Windows and Linux complexity requirements to maintain the security and integrity of passwords.	Interviewed the Compliance Analyst and determined password length and complexity requirements are controlled in Windows servers by GPOs and per-machine in Linux configurations Observed a screenshot of the Domain Admin 60-Day Password Policy and verified it specifies that elevated account passwords must be changed after 60 days and must be at least 10 characters in length Observed a sample of Linux machines match in comparison to a screenshot Linux configurations and verified a 15 character minimum and Linux-standard complexity	No Relevant Exceptions Noted
6.5	The organization has a process for assigning first-time passwords to new users.	Reviewed the Password Policy (dated April 6, 2020) and the Onboarding Policy (dated March 19, 2020) Interviewed the Compliance Analyst and determined the Internal IT staff sits with new employees and sets-up their first password; after a short training session, the Internal IT staff member changes the change password screen and forces the user to enter their new password; the Internal IT team member then verifies that the user with a new password can log in; if virtual is required, it is completed via virtual meeting with cameras enabled; and the Internal IT personnel transfer control of their system to allow the user to type in their own password Observed environments are capable of being set to force change upon login	No Relevant Exceptions Noted

6.6	Internal IT is responsible for resetting passwords for existing users.	Reviewed the Password Policy (dated April 6, 2020) and verified it clearly defines and limits responsibility for resetting passwords Interviewed the Compliance Analyst and the Director of Internal IT and determined that only Internal IT can reset passwords Observed appropriate personnel have access and understand responsibility for resetting passwords Observed ticket evidence that virtual meetings are used to validate identity during password reset during work-from-home (WFH) periods and verified that the small environment allows personal knowledge of users requesting password resets by staff responsible for verifying identity	No Relevant Exceptions Noted
6.7	The organization's Termination Policy requires access to be immediately revoked following termination.	Reviewed the Termination Policy (dated April 6, 2020) and verified that access must be immediately revoked for any terminated/separated employees and specifies account removal must be tracked via ticket in the ticketing system	No Relevant Exceptions Noted
6.8	The organization follows a termination checklist and uses tickets to revoke access for employees.	Interviewed the Compliance Analyst and determined that all terminations follow the Termination Checklist Observed checklist contains procedural/informational items (401k, COBRA), physical items (laptop, cell phone, badge), and requires an email to security and Internal IT Observed tickets created for sample subset of terminated/separated employees and verified evidence of removal of separated/terminated employees	No Relevant Exceptions Noted
6.9	The organization uses email requests and tickets to approve access and create new accounts.	Reviewed the Onboarding Policy, the Access Control Policy, the Employee New Hire Template, 2019 fourth quarter employee access reviews, and 2020 first quarter employee access reviews Interviewed the Compliance Manager, the Compliance Analyst, and the Director of Internal IT and determined that account	No Relevant Exceptions Noted

		creation is instigated by an HR email, and tickets are created and distributed Observed evidence of email requests and created tickets for new user authentication and verified manager approval is required for elevated access	
6.10	The organization has a process for removing accounts that have been inactive for 60 days.	Reviewed the 60-day review of users and vendors documentation (dated April 2020) Interviewed the Compliance Analyst and determined reports are run monthly for accounts that have been inactive for 60 more days, and tickets are created in response to the reports for disabling or removal of accounts Observed results of report being run and virtually observed tickets associated with account cleanup and verified that accounts that have been inactive for 60 days are disabled	No Relevant Exceptions Noted
6.11	Linux and Active Directory are used to enforce user, group, and domain policies on the system.	Reviewed a spreadsheet of Active Directory users, Active Directory groups, and GPO setting policies and verified policies are appropriate for passwords, including complexity, reuse, lockout on failure, and expiration first-time practices in Active Directory controllers Interviewed the Compliance Analyst regarding systems' users, groups, and domain policies and determined policies are captured in attached files and reviewed monthly Observed Linux password settings and verified they were configured similarly to Active Directory password settings	No Relevant Exceptions Noted
6.12	Passwords are required to be changed every 90 days.	Reviewed the Password Policy (dated April 6, 2020) and verified passwords must be changed at least once every 90 days Observed the Windows GPO settings and Linux settings and verified that user password parameters require users to change passwords/passphrases at least once every 90 days	No Relevant Exceptions Noted

6.13	The organization requires all passwords to be at least 10 characters in length.	Reviewed the Password Policy (dated April 6, 2020) and the Compliance Policy (dated June 2020) and verified that passwords must have at least 10 characters Interviewed the Compliance Analyst and determined the password length and complexity requirements are controlled in Windows servers by GPOs and per-machine in Linux configurations Observed a screenshot of the Active Directory domain password policy and verified that passwords must have at least 10 characters Observed a sample of Linux machines and verified they are configured to have passwords that contain at least 15 characters	No Relevant Exceptions Noted
6.14	The organization requires that passwords be composed a combination of numeric, alphabetic, and special characters.	Reviewed the Password Policy (dated April 6, 2020) and the Compliance Policy (dated June 2020) and verified that passwords must contain one numeric, one special character, one upper-case, and one lower-case character Interviewed the Compliance Analyst and determined the password length and complexity requirements are controlled in Windows servers by GPOs and per-machine in Linux configurations Observed a screenshot of the Active Directory domain password policy and verified that passwords must have at least 10 characters and standard Windows complexity requirements Observed a sample of Linux machines and verified they are configured to have passwords that contain at least 15 characters and Linux-standard complexity	No Relevant Exceptions Noted
6.15	The organization's Password Policy requires that the previous 24 passwords be remembered and cannot be reused.	Reviewed the Password Policy (dated April 6, 2020) and verified that the previous 24 passwords they cannot be reused Observed a screenshot of the Active Directory domain password policy and	No Relevant Exceptions Noted

		verified that the previous 24 passwords are remembered	
6.16	Linux and Active Directory are configured to lock out following failed authentication attempts.	Interviewed the Compliance Analyst and determined Windows settings are controlled via global policies, and Linux is controlled on a per-machine bases Observed that Active Directory policies specify a lockout of five failed attempts with a 30 minute lockout that requires contacting Internal IT to reset before that 30 minute timeout Observed a screenshot of Linux account settings against a sample of Linux boxes and verified that accounts are configured to lock out for 60 minutes after five failed passwords	No Relevant Exceptions Noted
6.17	The organization uses Active Directory and Linux as its primary logical access control system.	Reviewed the Remote Access Policy (dated April 6, 2020) and the User Account Policy (dated April 6, 2020) and verified that access requirements are documented Interviewed the Compliance Analyst and determined multiple systems are in use that provide logical access control Observed all access to sensitive systems is via virtual private network (VPN) with multi-factor authentication enabled and verified individual accounts are created for all users in both Active Directory and Linux, where root cannot be logged into directly Observed logs are sent to SIEM system and monitored at the SOC, group policies and system configuration standards enforce screen locking and system timeouts, and firewalls are configured with a default-deny ruleset and reviewed quarterly	No Relevant Exceptions Noted
6.18	Windows and Linux are configured to enforce session timeouts following idle periods.	Interviewed the Compliance Analyst and determined timeouts are specified in domain policy for Windows and per-machine in Linux Observed via virtual onsite that Linux machines are configured to lock out after 15 minutes of inactivity	No Relevant Exceptions Noted

		Observed Active Directory policies and verified it specifies a 15 minute screen lock timeout for Windows machines	
6.19	The organization uses Active Directory to ensure that application IDs can only be used by their respective application.	Reviewed the User Account Policy (dated April 6, 2020) and the Service Accounts Policy (dated April 6, 2020) and verified service account requirements are documented Interviewed the Compliance Analyst and determined that all service accounts are maintained through Active Directory, governed by the Service Accounts Policy, and limited in access to only access required for functionality Observed Active Directory service accounts are documented, limited in access, and reviewed frequently	No Relevant Exceptions Noted
6.20	The organization maintains policies that define how clients are registered and de-registered.	Reviewed the Creating Customer Portal Users document and verified the organization maintains procedures for registering and deregistering client accounts Observed an add user ticket, a customer order ticket, and a ticket to remove a user and verified that tickets are used to document account creation in accordance with policy	No Relevant Exceptions Noted
6.21	The organization has job classifications that define access for all systems used.	Reviewed job descriptions for personnel and verified that they address job responsibilities Interviewed the Compliance Analyst and determined that permissions in Active Directory correspond to an individual's job responsibilities Observed that Active Directory roles are tied to job descriptions and assigned appropriately Observed that the organization forbids ad hoc permissions and requires management approval to change accesses associated with a role	No Relevant Exceptions Noted
6.22	The organization maintains policies that require the use of unique user IDs and forbid sharing account information.	Reviewed the Service Accounts Policy (dated April 6, 2020), the User Account Policy (dated April 6, 2020), the Remote	No Relevant Exceptions Noted

		Access Policy (dated April 6, 2020), and the Password Policy (dated April 6, 2020) and verified they forbid sharing of accounts or passwords, limit usage and access of service accounts, and require role-based access grants to accounts Interviewed the Compliance Manager and the Compliance Analyst and determined that the organization maintains policies that require the use of unique user IDs	
6.23	The organization requires the use of multi-factor authentication for remote network access.	Reviewed the Remote Access Policy (dated April 6, 2020) and the Multi-Factor Authentication Policy (dated April 6, 2020) and verified that multi-factor authentication is required for remote access Observed during virtual onsite the use of multi-factor authentication for system access in multiple cases Observed network diagrams showing all servers that contain, process, or transmit sensitive data and verified they are in a network zone where multi-factor authentication is required to access	No Relevant Exceptions Noted
Control Objective 6 Conclusion: Based on the tests of operating effectiveness, the controls described above provide reasonable assurance that logical access to programs, data, and operating systems is restricted to authorized personnel.			

Control Objective 7 – Network Monitoring			
Control Objective 7: Controls provide reasonable assurance that network security and monitoring procedures are in place to identify and report unauthorized access attempts.			
Ctrl #	Controls Specified by Company	Testing Performed by Service Auditor	Test Results
7.1	The organization uses QRadar as its primary network logging tool to detect anomalies.	Reviewed the Logging and Monitoring Policy (dated April 6, 2020) and verified that logging requirements are formally documented Interviewed the Compliance Analyst and the SOC Manager and determined logging is collected by QRadar for all systems Observed raw logs, compiled dashboard, and reports from QRadar and verified that logs are gathered and retained Observed a sample subset of devices pulled from provided hardware inventory, including servers and network devices, and verified they are reporting logs to QRadar Observed logs for devices from multiple times within the audit period and verified that logs and drill-down events on dashboards contain protocol type, timestamp, source and destination IP, and port information	No Relevant Exceptions Noted
7.2	The organization participates in live monitoring of alerts in the SOC.	Reviewed the Logging and Monitoring Policy (dated April 6, 2020) and verified the log review requirements are documented Interviewed the Compliance Analyst and determined log reports are generated and reviewed, and live monitoring in the SOC is the primary method of log review Observed logs are all sent immediately to the QRadar and verified it provides an active alert monitoring dashboard that is always monitored in the SOC Observed continuous monitoring of the environment, including physical and logical	No Relevant Exceptions Noted

		in the NOC and SOC by live employees, and verified the acknowledgement of alerts Observed monthly reports that are provided to management	
7.3	QRadar retains logs are for at least one year.	Reviewed the Logging and Monitoring Policy (dated April 6, 2020) and the Backup and Recovery Policy (dated March 31, 2020) and verified retention requirements are addressed Observed the collection and retention of logs within QRadar for at least one year Observed log screenshots and verified that the last three months' worth of logs are immediately available for analysis in QRadar	No Relevant Exceptions Noted
7.4	The organization uses the SolarWinds tool and generates reports to monitor system capacity and plan for future requirements.	Interviewed the Compliance Analyst and determined system availability and service-level agreements (SLAs) are included in the organization's contracts with their customers; system capacity is discussed monthly at team meetings; the NOC uses tools, including SolarWinds, to monitor circuits, storage, and CPU utilization; and customer availability reports are provided to the organization's customers on a monthly basis Observed samples of customer availability reports and screenshot captures of NOC dashboard used to monitor disk space and system utilization	No Relevant Exceptions Noted
7.5	The organization performs monitoring activities to limit information leaks.	Reviewed the Logging and Monitoring Policy (dated April 6, 2020) and verified requirements for limiting information leakage are documented and in place Interviewed the Compliance Analyst and determined that the tool in use is QRadar Observed the QRadar console is always monitored by SOC staff and verified tickets are created in response to monitoring systems	No Relevant Exceptions Noted

7.6	The organization has implemented monitoring and intrusion-detection systems (IDS) to detect threats against systems that store, process, or transmit sensitive information.	Reviewed the Connectria Incident Response Plan (dated February 28, 2020) and the Incident Response Procedures (dated February 28, 2020) and verified requirements for monitoring IDS are documented Interviewed the Compliance Analyst and determined antivirus, file-integrity monitoring, IDS, and SIEM are always live-monitored by the SOC Observed virtually evidence of remote monitoring by SOC personnel Observed sampled subset of tickets created from incidents and verified follow-up responses were completed	No Relevant Exceptions Noted
7.7	The organization uses a Network Time Protocol (NTP) to ensure time synchronization.	Interviewed the Compliance Analyst and determined all servers in the environment are synchronized to Infoblox via NTP Observed a screenshot of NTP servers and keys and a sample subset of server configurations reflecting NTP configured and verified Infoblox is used as the authoritative time source	No Relevant Exceptions Noted
7.8	Personnel with access to QRadar are able to review audit trail files.	Interviewed the Compliance Manager and determined all employees with access to QRadar can view logs Observed audit logs are immediately relayed to SIEM (QRadar) and stored in protected mode on the QRadar servers Observed a list of employees with access to modify/delete logs in QRadar and verified it correlates with role-based need	No Relevant Exceptions Noted
Control Objective 7 Conclusion: Based on the tests of operating effectiveness, the controls described above provide reasonable assurance that network security and monitoring procedures are in place to identify and report unauthorized access attempts.			

Control Objective 8 – Configuration Management

Control Objective 8: Controls provide reasonable assurance that systems are configured in accordance with documented standards to identify and report unauthorized changes.

Ctrl #	Controls Specified by Company	Testing Performed by Service Auditor	Test Results
8.1	The organization's Change Management Policy and Procedures outline how changes are planned, communicated, evaluated, and implemented.	Reviewed the Change Management Policy and Procedures (dated April 8, 2020) and verified the following topics are covered: • Roles and responsibilities for CAB, Change Managers, Change Advisors, Change Sponsors, Change Requestors, and Change Implementers • Types of Changes (standard, minor, major, emergency) • Testing • Communication of changes • Evaluating risk of changes Interviewed the Compliance Analyst regarding Connectria's procedures to manage technology-related changes to its computing environments and determined the management of changes requires planning for the changes, communication of the changes, evaluating the risk of the changes, proper scheduling of the changes, and follow-up and learning from the changes Observed a 10% sample of firewall and non-firewall change tickets and verified changes are logged, prioritized, assigned, tested when possible, and communicated	No Relevant Exceptions Noted
8.2	The organization maintains formally documented system configuration standards that are based on industry-accepted standards.	Reviewed the Border Router Configuration Policy (dated April 20, 2020), the Browser Configuration Policy (dated April 6, 2020), the Firewall Configuration Policy (dated April 17, 2020), the IDS/IPS Configuration Policy (dated March 20, 2020), the Internal Router Configuration Policy (dated April 17, 2020), the SQL Server Policy (dated April 13, 2020), and the Security Program (dated March 3, 2020) and verified configuration standards are based on NIST special publications, PCI DSS requirements, and other security frameworks	No Relevant Exceptions Noted

		Reviewed the Appendix A of the Security Program (dated March 3, 2020) and verified that references to NIST publications are used as guidance for security hardening Interviewed the Compliance Analyst and determined system configuration policies are reviewed annually at a minimum and follow industry best practices and IT security frameworks, including ISO 27001, HIPAA, PCI DSS, HITRUST, and NIST SP 800-53	
8.3	The organization updates configuration standards quarterly based on the results of vulnerability scans.	Reviewed the Operating System Hardening Policy (dated February 28, 2020) and verified hardening standards are defined for web, email, database, infrastructure management, and file servers Interviewed the Compliance Analyst regarding the configuration responsibilities for personnel and determined the Security Team maintains configuration standards, the Compliance Team scans new operating system configuration and changes, and the OS Team mitigates discovered vulnerabilities Observed the Compliance Team runs quarterly vulnerability scans and resulting tickets from any identified concerns require remediation and verified configuration standards and hardened images are updated as appropriate, based on the scan results and corresponding tickets Observed results of recent internal and external penetration tests and internal and external vulnerability scans and verified configurations are up to date	No Relevant Exceptions Noted
8.4	Personnel with system configuration responsibilities receive technical certifications to ensure that they remain aware of the appropriate ways to securely configure systems.	Reviewed the current Certification List (dated April 22, 2020) and verified certifications are tracked, including the expiration date, to ensure all staff maintain their certifications as appropriate Interviewed the Compliance Manager regarding training attended by technical and security staff and determined that	No Relevant Exceptions Noted

		certifications obtained by staff are logged for each individual with system configuration responsibilities Observed the technical certifications list consists of certifications issued by recognized bodies, including AWS, ITIL, VMware, Microsoft, ISC2, Veeam, RedHat, and various vendors, and the list includes name of the certification or educational degree obtained	
8.5	The organization has a process in place to ensure that changes that affect system availability are communicated to relevant users.	Reviewed the Communication of Changes section of the Change Management Policy and Procedures document (dated April 8, 2020) and verified the policy describes how participants and/or affected business units are made aware of the change through normal project/activity communications prior to the change being presented for scheduling to the CAB and prior to change implementation Interviewed the Compliance Manager regarding the change management process and determined it includes communication of the changes to those who may be impacted Observed a sample of email notifications to management and users and verified they provided change information, such as the maintenance window, system impacted, and users who may be impacted	No Relevant Exceptions Noted
8.6	The organization maintains a Firewall Configuration Policy that requires quarterly review of firewall rules.	Reviewed the Firewall Configuration Policy (dated April 17, 2020) and verified it requires firewall rules to be reviewed quarterly and have justification for the rules that are configured Interviewed the Compliance Analyst and determined firewall and router configurations are reviewed quarterly, the Nipper Studio solution is used to facilitate the analysis of rule sets and identify potential security issues, and tickets are created that list the Nipper scans performed and issues found	No Relevant Exceptions Noted

		Observed two quarterly firewall review tickets and verified Nipper is run against firewalls and routers in-scope, and issues found are documented for review and remediation Observed findings in the Nipper scans are listed as "Critical" or "High" and documented in the Nipper Scan Exception (Critical & High)" document	
Control Objective 8 Conclusion: Based on the tests of operating effectiveness, the controls described above provide reasonable assurance that systems are configured in accordance with documented standards to identify and report unauthorized changes.			

Control Objective 9 – Vulnerability Management

Control Objective 9: Controls provide reasonable assurance that systems, processes, and software are tested periodically to ensure that security is maintained over time and after any changes.

Ctrl #	Controls Specified by Company	Testing Performed by Service Auditor	Test Results
9.1	The organization requires antivirus software definitions remain up to date.	Reviewed the Antivirus/Malware Policy (dated March 30, 2020) and the Vulnerability Management Policy (dated April 10, 2020) and verified that the organization automatically updates malicious code and spam protection mechanisms, including signature definitions Interviewed the Compliance Analyst and determined antivirus is installed on all machines, and Trend, Sophos, and Symantec report non-compliant machines to the SOC Observed a sample set of machines for antivirus configuration and verified that users cannot disable antivirus and definitions are automatically updated Observed antivirus reports for a three month period during the audit period and verified antivirus is installed and updated on both Windows and Linux servers Observed the logs being directed to QRadar and verified it's configured to generate alerts on non-compliant machines, and logs are stored for in excess of 12 months	No Relevant Exceptions Noted
9.2	The organization maintains patch management policies and procedures that define the use of sources for remediating vulnerabilities.	Reviewed the Patch Management Policy (dated April 13, 2020) and the Patching Procedures (dated April 10, 2020) and verified it defines requirements for identifying new security vulnerabilities, assigning a risk ranking to vulnerabilities that includes identification of all "high risk" and "critical" vulnerabilities, and using reputable outside sources for security vulnerability information Interviewed the Compliance Analyst and determined the hardware and software	No Relevant Exceptions Noted

		inventory lists are used to determine vendors that must be monitored Observed the internal and external vulnerability scans and penetration test and verified the findings of the identified vulnerabilities and traced the vulnerabilities from the scan to a trouble ticket through the engineering review and the closure of proper closure of the ticket	
9.3	The organization's Patching Procedures require that critical patches be installed within 30 days.	Reviewed the Patch Management Policy (dated April 13, 2020) and the Patching Procedures (dated April 10, 2020) and verified security patching is implemented on a monthly basis, which includes all critical security patches installed within 30 days and all important security patches installed within 90 days Interviewed the Compliance Analyst and determined all servers, workstations, applications, and/or network devices that process, store, or view confidential data are being patched on a regular basis Observed a sample set of machines and verified they have the most current patches Observed dashboard showing current patching and missing patch reports	No Relevant Exceptions Noted
9.4	The organization maintains policies that address requirements for vulnerability assessments and managing security risks.	Reviewed the Vulnerability Management Policy (dated April 10, 2020), the Vulnerability Scanning Procedure (dated April 10, 2020), and the Network Methodology Testing Policy (dated February 26, 2020) and verified that they address requirements for managing security risks Interviewed the Compliance Analyst and determined a vulnerability assessment is completed monthly and any issues found are communicated to the system owners via a ticket Observed a sample of vulnerability reports for a month during the audit period and the associated tickets for samples and verified	No Relevant Exceptions Noted

		the process is consistent with policies and processes	
9.5	The organization requires the use of outside resources to identify new security vulnerabilities.	Reviewed the Patching Procedure (dated April 10, 2020) and the Vulnerability Management Policy (dated April 10, 2020) and verified they require outside sources and monthly scans Interviewed the Compliance Analyst and determined Tripwire IP360, Tripwire Security Intelligence Hub, and IBM BigFix are all used as outside sources Observed via virtual onsite the use of Tripwire IP360, Tripwire Security Intelligence Hub, and IBM BigFix	No Relevant Exceptions Noted
9.6	The organization conducts scans following a significant change to the network.	Reviewed the Network Methodology Testing Policy (dated February 26, 2020) and the Vulnerability Scanning Procedure (dated April 10, 2020) and verified it requires a rescan of the environment after any significant change Interviewed the Compliance Manager and determined the organization has policies that require internal and external vulnerability scans after any significant change, and that the organization has had no significant environmental, staff, or scope changes within the audit period	No Relevant Exceptions Noted
9.7	The Data Classification/Ownership Policy classifies data into one of the following categories: Secret Confidential Internal Public	Reviewed the Data Classification/Ownership Policy (dated April 6, 2020) and verified the policy follows HITRUST and PCI DSS requirements and that data be categorized in one of four sensitivity classifications with separate handling requirements defined by minimum security baselines: Secret, Confidential, Internal, and Public Interviewed the Compliance Analyst and determined servers holding encrypted PHI are tagged accordingly, and all other in-scope data are classified as internal Observed business operations and operational procedures and verified data is stored and handled according to the	No Relevant Exceptions Noted

		corresponding classification security requirements	
9.8	The organization encrypts data to ensure it is secured prior to transmission across public networks.	Reviewed the Encryption and Hashing Policy (dated March 3, 2020) and verified it requires a secure method for key storage and transfer, mandated use of Perfect Forward Secrecy (PFS), strong protocols and ciphers, and secure hashing algorithms Observed evidence of backup settings, including AES 256 encryption for backups	No Relevant Exceptions Noted
9.9	The Cryptographic Key Management Policy addresses requirements for managing encryption keys.	Reviewed the Cryptographic Key Management Policy (dated April 30, 2020) and verified the policy acknowledges cryptographic keys as the most sensitive type of data, limits who can access and manage them, and establishes a limited lifespan for keys Interviewed the Compliance Analyst and determined the organization adheres to policies when managing encryption keys	No Relevant Exceptions Noted
9.10	The organization requires all data to be encrypted while at rest within the environment.	Reviewed the Encryption and Hashing Policy (dated March 3, 2020) and the Backup and Recovery Policy (dated March 31, 2020) and verified that all covered information must be rendered unusable, unreadable, or undecipherable where stored Interviewed the Compliance Analyst and determined backups are encrypted in accordance with the Backup and Recovery Policy Observed evidence of backups being encrypted in all cases	No Relevant Exceptions Noted
9.11	Customers are required to determine data retention requirements, and the organization maintains policies that define accommodations for requirements.	Reviewed a variety of policies and contracts and verified that the business model requires that customers own their data and must understand and require any retention policies that accommodate regulatory or legal requirements, statements of work define requirements from the customer to the organization, and the organization's policies accommodate these needs	No Relevant Exceptions Noted

		Interviewed the Compliance Analyst and determined regulatory, legal, and business requirements are documented and in place	
9.12	The information involved in application service transactions is encrypted to ensure the data is protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication, or replay.	Reviewed the Encryption and Hashing Policy (dated March 3, 2020) and verified it requires a secure method for key storage and transfer, mandated use of PFS, strong protocols and ciphers, and secure hashing algorithms, and it requires encryption at rest, in transit, and in logs Interviewed the Compliance Manager and determined the organization is not involved in the configuration of the customer systems/applications that transmit, route, message, disclose, duplicate or replay, and this is managed and configured by the customers and the applications that they use Observed during virtual onsite evidence of encryption at rest and encryption during internal communications while onsite	No Relevant Exceptions Noted
Control Objective 9 Conclusion: Based on the tests of operating effectiveness, the controls described above provide reasonable assurance that systems, processes, and software are tested periodically to ensure that security is maintained over time and after any changes.			

Control Objective 10 – Backup and Restoration

Control Objective 10: Controls provide reasonable assurance that backups of data and system files are regularly created, and that archived data is available for restoration in the event of processing errors.

Ctrl #	Controls Specified by Company	Testing Performed by Service Auditor	Test Results
10.1	The organization conducts backup processes that includes writing backups to tape and storing them in Iron Mountain.	Reviewed the Backup and Recovery Policy (dated March 31, 2020) and verified that data backup procedures are in place Interviewed the Compliance Analyst and the Team Lead of Data Protection and determined backups are taken daily and written to tape, and the tapes are stored and retained by Iron Mountain Observed configurations and verified that backups are taken as full backups daily and written to tape Observed records showing transactions providing tapes to Iron Mountain for transport/storage Observed portal records showing location and content of tapes by barcode number as well as data owners Observed records of backup recoveries within the audit period Observed that the organization obtained SOC reports for Wasabi, which is used for offsite backup storage	No Relevant Exceptions Noted

Control Objective 10 Conclusion: Based on the tests of operating effectiveness, the controls described above provide reasonable assurance that backups of data and system files are regularly created, and that archived data is available for restoration in the event of processing errors.

Control Objective 11 – Business Continuity and Disaster Recovery

Control Objective 11: Controls provide reasonable assurance that the organization is able to maintain or recover business-critical processing capabilities in the event of the loss of a facility or a major system failure.

Ctrl #	Controls Specified by Company	Testing Performed by Service Auditor	Test Results
11.1	The organization has implemented plans to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.	Reviewed a Connectria Master Services Agreement (dated March 13, 2020) and verified Connectria is not responsible or liable for any damages, delays, or other failures to fulfill their obligations as a result of events or circumstances beyond their reasonable control including, without limitation, delays due to natural disaster, public health emergencies, epidemics, pandemics, and/or other occurrences whether or not similar to those listed above Reviewed the Connectria Business Continuity Plan (dated March 17, 2020), the Business Resumption Plan (dated February 28, 2020), and the Business Impact Analysis (dated March 17, 2020) and verified they address appropriate topics, including scope and goals, responsibilities, critical functions, emergency response, recovery steps, and training and testing Interviewed the Compliance Manager regarding the two types of continuity plans continually updated by operations management: • The Technology Services Recovery Plan, which covers computer operations, infrastructure segments, and all server-based applications • The Business Resumption Plan, which covers all other departments within Connectria and defines procedures the case of problems, emergencies, or disasters, including loss of computer operations Observed business resumption plans are based on results of BIA for current business operations and critical associated support functions	No Relevant Exceptions Noted

		Observed results of recent tabletop exercise and verified continuity plans are updated based on lessons learned from the test (e.g., pandemic response)	
11.2	Business continuity plans are reviewed, tested, and updated annually.	Reviewed the Connectria Business Continuity Plan (dated March 17, 2020) and verified the plan requires annual testing of the business continuity and business resumption plans Reviewed the Business Continuity Plan and verified a test was performed in March 2020, which covered scenarios based on a COVID-19 pandemic Interviewed the Compliance Manager regarding the testing and updating of business continuity plans and determined tabletop exercises are performed annually based on specific scenarios, and plans are updated with lessons learned as appropriate Observed results of the recent tabletop exercise and verified business continuity and resumption plans were updated based on lessons learned from the test	No Relevant Exceptions Noted
Control Objective 11 Conclusion: Based on the tests of operating effectiveness, the controls described above provide reasonable assurance that is able to maintain or recover business-critical processing capabilities in the event of the loss of a facility or a major system failure.			

Control Objective 12 – Vendor Management			
Control Objective 12: Controls provide reasonable assurance that vendors are appropriately vetted, approved, and monitored to define the services provided and limit third-party access to sensitive data.			
Ctrl #	Controls Specified by Company	Testing Performed by Service Auditor	Test Results
12.1	The organization's Vendor Risk Assessment Policy defines due diligence procedures that are completed prior to engaging with service providers.	Reviewed the Vendor Risk Assessment Policy (dated February 28, 2020) and verified vendor risks are examined to consider the following: • The type of access the external party will have to the information and information asset(s) • Practices and procedures to deal with security incidents and potential damages, and the terms and conditions for the continuation of external party access in the case of a security incident • Legal and regulatory requirements and other contractual obligations relevant to the external party, which must be taken into account Interviewed the Compliance Analyst regarding the organization's documented framework for managing the lifecycle of vendor relationships and determined a risk analysis is conducted for each potential vendor, and the risk analysis utilizes the Vendor Risk Rating Matrix to assign a vendor risk rating of low, medium, or high	No Relevant Exceptions Noted
12.2	Managers are responsible for following vendor management policies to ensure that third parties are maintaining compliance and effectively carrying out contracts.	Reviewed the Vendor Risk Assessment Policy (dated February 28, 2020), the Vendor Management Policy (dated March 5, 2020), and the Contract Management Policy (dated February 28, 2020) and verified the policies specify the responsibilities for subject area managers Interviewed the Compliance Analyst and determined each manager is responsible for following the vendor management policies for vendor assessment and evaluating them for security risks and maintaining the contracts	No Relevant Exceptions Noted

12.3	The organization requires all third parties to sign a non-disclosure agreement prior to sharing information with them.	Reviewed non-disclosure agreements and verified standard NDA language is used to protect confidential information and restrict disclosure to other third parties, unless the other party's written consent has been obtained, and the agreement termination conditions are defined in the NDA language as well as governing law and injunctive relief Interviewed the Compliance Analyst and determined the use of Mutual Non-Disclosure Agreements with third parties whenever either party may need to disclose certain confidential or proprietary information to the other parties	No Relevant Exceptions Noted
12.4	The organization obtains and reviews audit reports from critical vendors and service providers.	Observed that the organization obtained third-party assessment reports from the following vendors to support vendor management efforts: • Netrality Properties • CyrusOne, LLC • 365 Data Centers • Equinix • Iron Mountain	No Relevant Exceptions Noted
Control Objective 12 Conclusion: Based on the tests of operating effectiveness, the controls described above provide reasonable assurance that vendors are appropriately vetted, approved, and monitored to define the services provided and limit third-party access to sensitive data.			