Connectria, LLC

FISMA Compliance Audit Report

Based on NIST SP 800-171

September 30, 2020

KirkpatrickPrice

4235 Hillsboro Pike
Suite 300
Nashville, TN 37215

TABLE OF CONTENTS

4235 Hillsboro Pike, Suite 300
Nashville, TN 37215

Richard S. Waidmann
CEO
Connectria, LLC
10845 Olive Boulevard, Suite 300
St. Louis, Missouri 63141

Dear Richard S. Waidmann,

We have completed a compliance audit on the Federal Information Security Management Act of 2002 (FISMA) for Connectria, LLC in St. Louis, Missouri. The audit used the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171.

It is our hope that, as a result of this audit, we are providing recommendations for strengthening the company's information system and the management, administrative, technical, and physical safeguards employed to protect the confidentiality of the system and its information. This report contains the findings for the purposes of verifying compliance with regulatory requirements for FISMA and of evaluating the development and implementation of controls as part of the ongoing compliance plan. Each finding references the evidentiary documentation gathered during the audit.

Based on our objective analysis, we determined that Connectria, LLC has implemented safeguards that meet the protections required by FISMA, and the information security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of nonpublic personal information is protected as of September 30, 2020.

This report may be shared with client organizations, so they may view the results in the context of industry risk management. Please contact us with any questions about the procedures, testing, or sampling performed.

Respectfully submitted,

Joseph Kirkpatrick
CPA, CISSP, CGEIT, CISA, CRISC, QSA

EXECUTIVE SUMMARY

Our examination of the security requirements that follow are based on NIST (National Institute of Standards and Technology) Special Publication 800-171. NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all U.S. federal agency operations and assets. The goal is to assist federal agencies in implementing the Federal Information Security Modernization Act (FISMA) of 2014 and to protect their information and information systems. However, the guidelines developed by NIST are not just for federal agencies but are designed to be used as guidance to protect Controlled Unclassified Information (CUI) within the information systems of nonfederal organizations.

KirkpatrickPrice has performed an audit of Connectria, LLC's compliance with the NIST security controls deemed applicable to the information system. We noted that Connectria, LLC's management has demonstrated a commitment to FISMA compliance and consistent adherence to the implementation of best practices as it applies to information security. We also wish to note that the NIST standards comprise a set of guidelines for organizations to improve their security control environment. It is not necessary, nor is it practical, for all NIST controls to be implemented. Some of the FISMA-related requirements expressed in the NIST standards and guidelines are uniquely federal. Other controls do not directly relate to protecting the confidentiality of CUI or are expected to be routinely satisfied by nonfederal organizations without specification.

Our overall audit revealed that Connectria, LLC has adequately addressed the significant security requirements deemed necessary to protect controlled unclassified information. However, we provide the below findings and recommendations to strengthen the security environment.

Noted Deficiencies

None
No deficiencies were found.

METHODOLOGY

During the audit, the auditor performed information-gathering via KirkpatrickPrice's proprietary online portal, an onsite visit to the corporate administrative site and the data center site, interviews with relevant personnel, reviews of corporate and departmental policies and procedures, direct observations of processes and system configuration, and physical inspection of various control implementations. The auditor obtained data from the Human Resources, Security and Compliance, Information Technology, and Application Development departments and conducted interviews with senior management.

NIST controls are organized into fourteen families. The families are closely aligned with the minimum-security requirements published in NIST 800-53. The controls have been tailored within NIST 800-171 to apply to CUI. The table below summarizes the families in the NIST security control catalog that apply to the protection of CUI.

Security Requirement Families

Families	
Access Control	Media Protection
Awareness and Training	Personnel Security
Audit and Accountability	Physical Protection
Configuration Management	Risk Assessment
Identification and Authentication	Security Assessment
Incident Response	System and Communications Protection
Maintenance	System and Information Integrity

CONTROLS IN SCOPE

Organizations are required to adequately mitigate the risk arising from use of information and information systems in the execution of missions and business functions. A significant challenge for organizations is to determine the appropriate set of security controls, which if implemented and determined to be effective, would most cost-effectively mitigate risk while complying with the security requirements defined by applicable federal laws, executive orders, directives, policies, standards, or regulations.

Security controls as defined in the NIST security control baseline represent an information system-wide set of controls that may not be necessary or applicable to every component in the system. Security controls are applicable only to the components of the information system that provide or support the security capability addressed by the control and are sources of potential risk being mitigated by the control. For example, auditing controls are typically allocated to components of an information system that provide auditing capability (e.g. servers) and are not necessarily applied to every user-level workstation within the organization. Organizations assess the inventory of information system components to determine which security controls are applicable to the various components and subsequently make explicit decisions regarding where to allocate the controls in order to satisfy organizational security requirements.

Only the controls necessary to protect a moderate level of confidentiality of CUI were tested. The moderate security control baseline published within NIST Special Publication 800-53 was used as the starting point for tailoring actions. Other controls can and should be used within an information security system; however, these controls were not tested by KirkpatrickPrice.

Certain of the NIST 800-171 controls were deemed N/A for the following reasons:

N/A Controls

3.1.18
N/A: Mobile devices are not allowed on the internal LAN.
3.1.19
N/A: Mobile devices are not allowed on the internal LAN.
3.7.3
N/A: All devices within the in-scope network do not leave the data center.
3.13.13
N/A: Mobile code technologies are not used in this environment.
3.13.15
N/A: Connectria does not offer application development as a service to its customers.

NIST Security Control Descriptions and Gap Identification

ACCESS CONTROL

Access Control – Basic Security Requirements: 3.1.1
The organization limits information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
Testing Performed by Compliance Auditor
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 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
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 documented and requires that access be assigned based on role 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
Interviewed the Compliance Analyst and determined that all terminations follow termination checklists Observed checklist contains procedural/informational items (401k, COBRA), physical items (laptop, cell phone, badge), and requires and email to security and Internal IT Observed tickets created for a sample of terminated/separated employees and verified evidence of removal of separated/terminated employees
Reviewed the Service Accounts Policy (dated April 6, 2020), the User Account Policy (dated April 6, 2020), the Remote 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
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Access Control – Basic Security Requirements: 3.1.2
The organization limits information system access to the types of transactions and functions that authorized users are permitted to execute.
Testing Performed by Compliance Auditor
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 documented and requires that access be assigned based on role 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
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
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
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Access Control – Derived Security Requirements: 3.1.3
The organization controls the flow of CUI in accordance with approved authorizations.
Testing Performed by Compliance Auditor
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 portal tickets and verified the biannual review of the network diagram
Reviewed the Firewall Configuration Policy (dated April 17, 2020) and verified authorized protocols are defined and are restricted to specific hosts, and Connectria utilizes firewalls from at least two different vendors that employ stateful packet inspection Interviewed the Compliance Analyst and determined it is the responsibility of the Security and Compliance Group to create and maintain the security requirements for the configuration of firewalls Observed results of Nipper scans (2019 Q4 and 2020 Q1) and verified firewalls are scanned quarterly to ensure security requirements for Connectria's firewall configuration are maintained Observed the following change control tickets and verified any changes necessary to the firewall rules are documented and approved: • 2019 Q4 FW Review Ticket 462351 • 2020 Q1 FW Review Ticket 482526
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Access Control – Derived Security Requirements: 3.1.4
The organization separates the duties of individuals to reduce the risk of malevolent activity without collusion.
Testing Performed by Compliance Auditor
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
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Access Control – Derived Security Requirements: 3.1.5
The organization employs the principle of least privilege, including for specific security functions and privileged accounts.
Testing Performed by Compliance Auditor
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 documented and requires that access be assigned based on role 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
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
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
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Access Control – Derived Security Requirements: 3.1.6
The organization uses non-privileged accounts or roles when accessing non-security functions.
Testing Performed by Compliance Auditor
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 documented and requires that access be assigned based on role

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
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
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
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Access Control – Derived Security Requirements: 3.1.7
The organization prevents non-privileged users from executing privileged functions and audit the execution of such functions.
Testing Performed by Compliance Auditor
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 documented and requires that access be assigned based on role 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
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
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
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Access Control – Derived Security Requirements: 3.1.8
The organization limits unsuccessful logon attempts.
Testing Performed by Compliance Auditor
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
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Access Control – Derived Security Requirements: 3.1.9
The organization provides privacy and security notices consistent with applicable CUI rules.
Testing Performed by Compliance Auditor
Interviewed the Compliance Manager and determined that communication of the privacy requirements is effectively implemented during the audit period Observed Privacy Policy on the company website and verified the policy is available to employees and clients, and the policy addresses what is collected and how information may be used
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 IP360
- Veeam
- Confluence
- BigFix
- Trend Antivirus

Control Deficiencies Noted: YES ☐ NO ☒
If YES, explain the nature of the deficiency:

Access Control – Derived Security Requirements: 3.1.10
The organization uses session lock with pattern-hiding displays to prevent access/viewing of data after period of inactivity.
Testing Performed by Compliance Auditor
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 Observed Active Directory policies and verified it specifies a 15-minute screen lock timeout for Windows machines
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Access Control – Derived Security Requirements: 3.1.11
The organization terminates (automatically) a user session after a defined condition.
Testing Performed by Compliance Auditor
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 Observed Active Directory policies and verified it specifies a 15-minute screen lock timeout for Windows machines
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Access Control – Derived Security Requirements: 3.1.12
The organization monitors and controls remote access sessions.
Testing Performed by Compliance Auditor
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
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 of devices from the 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
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
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Access Control – Derived Security Requirements: 3.1.13
The organization employs cryptographic mechanisms to protect the confidentiality of remote access sessions.
Testing Performed by Compliance Auditor
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 of devices from the 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
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
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
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Access Control – Derived Security Requirements: 3.1.14
The organization routes remote access via managed access control points.
Testing Performed by Compliance Auditor
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 Observed evidence of backup settings, including AES 256 encryption for backups
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
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
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Access Control – Derived Security Requirements: 3.1.15
The organization authorizes remote execution of privileged commands and remote access to security-relevant information.
Testing Performed by Compliance Auditor
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
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 Observed evidence of backup settings, including AES 256 encryption for backups
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Access Control – Derived Security Requirements: 3.1.16
The organization authorizes wireless access prior to allowing such connections.
Testing Performed by Compliance Auditor
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 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 and wireless access
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 documented and requires that access be assigned based on role 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
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Access Control – Derived Security Requirements: 3.1.17
The organization protects wireless access using authentication and encryption.
Testing Performed by Compliance Auditor
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
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 Observed evidence of backup settings, including AES 256 encryption for backups
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
Interviewed the Compliance Analyst and determined all cables are underground when possible and all termination points are in locked rooms, and power and data cables are separated Observed via virtual onsite that access to the facility is controlled by live security and cameras Observed network diagrams show no access from wireless network to management network
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Access Control – Derived Security Requirements: 3.1.18
The organization controls the connection of mobile devices.
Testing Performed by Compliance Auditor
N/A: Mobile devices are not allowed on the internal LAN.
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Access Control – Derived Security Requirements: 3.1.19
The organization encrypts CUI on mobile devices.
Testing Performed by Compliance Auditor
N/A: Mobile devices are not allowed on the internal LAN.
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Access Control – Derived Security Requirements: 3.1.20
The organization verifies and controls/limits connections to and use of external information systems.
Testing Performed by Compliance Auditor
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 of devices from the 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
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
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Access Control – Derived Security Requirements: 3.1.21
The organization limits use of organizational portable storage devices on external information systems.
Testing Performed by Compliance Auditor
Reviewed the Removable Media Policy (dated April 6, 2020) and verified it restricts the use of removable media on the organization's systems Interviewed the Compliance Analyst and determined there is a policy in place relative to handling print, digital, and removable media

Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Access Control – Derived Security Requirements: 3.1.22
The organization controls information posted or processed on publicly accessible information systems.
Testing Performed by Compliance Auditor
Reviewed the Security Program (dated March 3, 2020) and verified the 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
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 Observed the Confluence portal used by Connectria and verified policies are maintained and accessible to all employees
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

AWARENESS AND TRAINING

Awareness and Training – Basic Security Requirements: 3.2.1
The organization ensures that managers, systems administrators, and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of organizational information systems.
Testing Performed by Compliance Auditor
Reviewed the Security Program (dated March 3, 2020) and verified the following 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
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Awareness and Training – Basic Security Requirements: 3.2.2
The organization ensures that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.
Testing Performed by Compliance Auditor
Reviewed the Security Program (dated March 3, 2020) and verified the following 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

Control Deficiencies Noted: YES ☐ NO ☒
If YES, explain the nature of the deficiency:

Awareness and Training – Derived Security Requirements: 3.2.3
The organization provides security awareness training on recognizing and reporting potential indicators of insider threat.
Testing Performed by Compliance Auditor
Reviewed the Security Program (dated March 3, 2020) and verified the following 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
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
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Audit and Accountability – Basic Security Requirements: 3.3.1
The organization creates, protects, and retains information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.
Testing Performed by Compliance Auditor
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
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 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 in the NOC and SOC by live employees, and verified the acknowledgement of alerts Observed monthly reports that are provided to management
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Audit and Accountability – Basic Security Requirements: 3.3.2
The organization ensures that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.
Testing Performed by Compliance Auditor
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 of devices from the 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
Reviewed a list of failed logins (dated November 18, 2019), the list of successful logins (dated April 11, 2020), the PCI successful logins (April 2020), and PCI host login failures (dated January 2020) Interviewed the Compliance Analyst and determined logs are maintained in QRadar for over one year, and all network devices and server logs are relayed immediately to the SIEM (QRadar) Observed evidence of log concatenation in QRadar Observed monthly reports that are delivered to management Observed logs from a random date within the audit period were immediately accessible and thorough
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Audit and Accountability – Derived Security Requirements: 3.3.3
The organization reviews and updates audited events.
Testing Performed by Compliance Auditor
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 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 in the NOC and SOC by live employees, and verified the acknowledgement of alerts Observed monthly reports that are provided to management
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Audit and Accountability – Derived Security Requirements: 3.3.4
The information system alerts in the event of an audit process failure.

Testing Performed by Compliance Auditor
Reviewed the Tripwire Report – AD-Detailed Changes (dated November 1, 2019), the Tripwire Report – AD-Detailed Changes (dated February 28, 2020), the PCI-OSSEC FIM System Changes (dated December 9-12, 2019), the PCI-Ossec FIM System Changes (dated March 9-16, 2020), and PCI Host Login Failure – OSSEC (dated January 1 – February 1, 2020) and verified file integrity changes are detected and analyzed Interviewed the Compliance Analyst and the SOC manager and determined OSSEC is used to monitor file integrity, and reports are provided to the SOC Observed evidence of daily review of file integrity reports
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Audit and Accountability – Derived Security Requirements: 3.3.5
The information system correlates audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity.
Testing Performed by Compliance Auditor
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 of devices from the 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
Reviewed a list of failed logins (dated November 18, 2019), the list of successful logins (dated April 11, 2020), the PCI successful logins (April 2020), and PCI host login failures (dated January 2020) Interviewed the Compliance Analyst and determined logs are maintained in QRadar for over one year, and all network devices and server logs are relayed immediately to the SIEM (QRadar) Observed evidence of log concatenation in QRadar Observed monthly reports that are delivered to management Observed logs from a random date within the audit period were immediately accessible and thorough
Control Deficiencies Noted: YES ☐ NO ☒

If YES, explain the nature of the deficiency:

Audit and Accountability – Derived Security Requirements: 3.3.6
The information system provides audit reduction and report generation to support on-demand analysis and reporting.
Testing Performed by Compliance Auditor
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 of devices from the 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
Reviewed a list of failed logins (dated November 18, 2019), the list of successful logins (dated April 11, 2020), the PCI successful logins (April 2020), and PCI host login failures (dated January 2020) Interviewed the Compliance Analyst and determined logs are maintained in QRadar for over one year, and all network devices and server logs are relayed immediately to the SIEM (QRadar) Observed evidence of log concatenation in QRadar Observed monthly reports that are delivered to management Observed logs from a random date within the audit period were immediately accessible and thorough
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Audit and Accountability – Derived Security Requirements: 3.3.7
The information system provides an information system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.
Testing Performed by Compliance Auditor
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 of server configurations reflecting NTP configured and verified Infoblox is used as the authoritative time source
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Audit and Accountability – Derived Security Requirements: 3.3.8
The information system protects audit information and audit tools from unauthorized access, modification, and deletion.
Testing Performed by Compliance Auditor
Interviewed the Compliance Manager and determined all employees with access to QRadar can view logs Observed audit logs are immediately relayed to the 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
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Audit and Accountability – Derived Security Requirements: 3.3.9
The information system limits management of audit functionality to a subset of privileged users.
Testing Performed by Compliance Auditor
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 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
Interviewed the Compliance Manager and determined all employees with access to QRadar can view logs Observed audit logs are immediately relayed to the 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
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Configuration Management – Basic Security Requirements: 3.4.1
The organization establishes and maintains baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.
Testing Performed by Compliance Auditor
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 of devices from the 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
Interviewed the Compliance Analyst and determined the system inventory is updated automatically using a portal solution 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
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
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 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
Reviewed the Change Management Policy and Procedures (dated April 8, 2020) and verified the following topics are covered: • Roles and responsibilities for change advisory board (CAB), change managers, change advisors, sponsors, requestors, and 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
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Configuration Management – Basic Security Requirements: 3.4.2
The organization establishes and enforces security configuration settings for information technology products employed in organizational information systems.
Testing Performed by Compliance Auditor
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, and they address the common hardening parameters in use, including networking/port controls, account, password, and user ID controls, and patching controls 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
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, sponsors, requestors, and 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

Control Deficiencies Noted: YES ☐ NO ☒
If YES, explain the nature of the deficiency:

Configuration Management – Derived Security Requirements: 3.4.3
The organization tracks, reviews, approves/disapproves, and audits changes to information systems.
Testing Performed by Compliance Auditor
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 Interviewed the Compliance Manager and determined Connectria's procedures for the CAB and the Sponsor to approve new systems
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, sponsors, requestors, and 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
Reviewed the Change Management Policy and Procedures and verified procedures define how changes are recorded, prioritized, approved, tested where possible, communicated to participants, evaluated for risks, and include back out plans

Interviewed the Compliance Analyst regarding the change review and approval process by change managers during CAB meetings and determined changes that do not meet requirements or have unacceptable levels of risk are put on hold pending further investigation Observed a sample of network and firewall change tickets (6 of 55) performed during the audit period and verified the changes followed the documented change procedures
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Configuration Management – Derived Security Requirements: 3.4.4
The organization analyzes the security impact of changes prior to implementation.
Testing Performed by Compliance Auditor
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, sponsors, requestors, and 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
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 Interviewed the Compliance Manager and determined Connectria's procedures for the CAB and the Sponsor to approve new systems
Reviewed the Change Management Policy and Procedures and verified procedures define how changes are recorded, prioritized, approved, tested where possible, communicated to participants, evaluated for risks, and include back out plans Interviewed the Compliance Analyst regarding the change review and approval process by change managers during CAB meetings and determined changes that do not meet requirements or have unacceptable levels of risk are put on hold pending further investigation Observed a sample of network and firewall change tickets (6 of 55) performed during the audit period and verified the changes followed the documented change procedures
Control Deficiencies Noted: YES ☐ NO ☒

If YES, explain the nature of the deficiency:

Configuration Management – Derived Security Requirements: 3.4.5
The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.
Testing Performed by Compliance Auditor
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 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 audit period
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, sponsors, requestors, and 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
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Configuration Management – Derived Security Requirements: 3.4.6
The organization employs the principle of least functionality by configuring the information system to provide only essential capabilities.
Testing Performed by Compliance Auditor
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 documented and requires that access be assigned based on role 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
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 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
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 the 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
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Configuration Management – Derived Security Requirements: 3.4.7
The organization restricts, disables, and prevents the use of nonessential programs, functions, ports, protocols, and services.
Testing Performed by Compliance Auditor
Reviewed firewall configurations, network diagrams, and data flow diagrams

Interviewed the Compliance Manager to discuss firewalls/routers have a default-deny approach with documented business cases for all open ports and protocols
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 the 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
Reviewed the Border Router Configuration Policy (dated April 20, 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 OS Hardening Policy (dated February 28, 2020) Interviewed the Compliance Analyst and determined hardening standards are built around business justification, and justification is evaluated at each review of hardening standards Observed evidence of frequent configuration review and approval Observed changes to firewalls, OS, and routers are tracked in change management system and business case is documented there
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Configuration Management – Derived Security Requirements: 3.4.8
The organization applies deny-by-exception (blacklist) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.
Testing Performed by Compliance Auditor
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 documented and requires that access be assigned based on role 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
Reviewed the Software Approval Policy (dated April 6, 2020) and verified the organization has implemented procedures to prevent the execution of unauthorized or blacklisted software on the information system Interviewed the Compliance Manager and determined FIM is in place watching for unauthorized software, and antivirus is watching for known malware. Observed SOC 24-hour monitoring while and evidence of SIEM collection/reportability and FIM functionality
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 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 the 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
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Configuration Management – Derived Security Requirements: 3.4.9
The organization controls and monitors user-installed software.
Testing Performed by Compliance Auditor
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 a non-login
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 IP360
- Veeam
- Confluence
- Trend Antivirus
- BigFix

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 of devices from the 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

Control Deficiencies Noted: YES ☐ NO ☒
If YES, explain the nature of the deficiency:

IDENTIFICATION AND AUTHENTICATION

Identification and Authentication – Basic Security Requirements: 3.5.1
The organization identifies information system users, processes acting on behalf of users, or devices.
Testing Performed by Compliance Auditor
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 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
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Identification and Authentication – Basic Security Requirements: 3.5.2
The organization authenticates (or verifies) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
Testing Performed by Compliance Auditor
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 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
Reviewed the Service Accounts Policy (dated April 6, 2020), the User Account Policy (dated April 6, 2020), the Remote 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
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Identification and Authentication – Derived Security Requirements: 3.5.3
The organization uses multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.
Testing Performed by Compliance Auditor
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
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
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Identification and Authentication – Derived Security Requirements: 3.5.4
The organization employs replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.
Testing Performed by Compliance Auditor
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
Reviewed the Multi-Factor Authentication Policy (dated April 6, 2020) Interviewed the Compliance Analyst and determined the organization uses MFA to supplement passwords for Cisco VPN connections to the sensitive data environments Observed use of MFA to augment password authentication to establish a connection to the sensitive data environment
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Identification and Authentication – Derived Security Requirements: 3.5.5
The organization prevents reuse of identifiers for a defined period.
Testing Performed by Compliance Auditor
Reviewed the Password Policy (dated April 6, 2020) and verified that the previous 24 passwords cannot be reused Observed a screenshot of the Active Directory domain password policy and verified that the previous 24 passwords are remembered
Reviewed the Service Accounts Policy (dated April 6, 2020), the User Account Policy (dated April 6, 2020), the Remote 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
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 camera evidence of asset tracking in the Confluence portal including nature of data, owner, date, and source
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Identification and Authentication – Derived Security Requirements: 3.5.6
The organization disables identifiers after a defined period of inactivity.
Testing Performed by Compliance Auditor
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 or 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
Reviewed the Service Accounts Policy (dated April 6, 2020), the User Account Policy (dated April 6, 2020), the Remote 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
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 camera evidence of asset tracking in the Confluence portal including nature of data, owner, date, and source
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Identification and Authentication – Derived Security Requirements: 3.5.7
The organization enforces a minimum password complexity and change of characters when new passwords are created.
Testing Performed by Compliance Auditor
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 verified that the previous 24 passwords are remembered
Reviewed the Password Policy (dated April 6, 2020) and the Compliance Policy (dated June 2020) and verified that passwords must contain at least 10 characters that contain a combination of 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
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Identification and Authentication – Derived Security Requirements: 3.5.8
The organization prohibits password reuse for a specified number of generations.
Testing Performed by Compliance Auditor
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 verified that the previous 24 passwords are remembered
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Identification and Authentication – Derived Security Requirements: 3.5.9
The organization allows temporary password use for system logons with an immediate change to a permanent password.
Testing Performed by Compliance Auditor
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
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
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Identification and Authentication – Derived Security Requirements: 3.5.10
The organization stores and transmits only encrypted representation of passwords.
Testing Performed by Compliance Auditor
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 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 of Linux configurations and verified a 15-character minimum and Linux-standard complexity
Reviewed the Password Policy (dated April 6, 2020) and verified it addresses both general policy and temporary password procedures, requires industry-standard complexity or better, specifies password expiration timelines and prevents password recycling, and forbids scripting or hard-coding of passwords, sharing of passwords, and applications that display passwords when entered Interviewed the Compliance Analyst and the Director Internal IT regarding the procedures the organization has implemented to maintain the security and integrity of passwords and determined a Password Policy is maintained, approved, and distributed, and the organization does not use electronic signatures or tokens for access
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Identification and Authentication - Derived Security Requirements: 3.5.11
The organization obscures feedback of authentication information.
Testing Performed by Compliance Auditor
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
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

INCIDENT RESPONSE

Incident Response – Basic Security Requirements: 3.6.1
The organization establishes an operational incident-handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.
Testing Performed by Compliance Auditor
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
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Incident Response – Basic Security Requirements: 3.6.2
The organization tracks, documents, and reports incidents to appropriate officials and/or authorities both internal and external to the organization.
Testing Performed by Compliance Auditor
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
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Incident Response – Derived Security Requirements: 3.6.3
The organization tests the organizational incident response capability.
Testing Performed by Compliance Auditor
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
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

MAINTENANCE

Maintenance – Basic Security Requirements: 3.7.1
The organization performs maintenance on organizational information systems.
Testing Performed by Compliance Auditor
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, sponsors, requestors, and 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
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
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Maintenance – Basic Security Requirements: 3.7.2
The organization provides effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

Testing Performed by Compliance Auditor
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
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 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
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Maintenance – Derived Security Requirements: 3.7.3
The organization ensures equipment removed for off-site maintenance is sanitized of any CUI.
Testing Performed by Compliance Auditor
N/A: All devices within the in-scope network do not leave the data center.
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Maintenance – Derived Security Requirements: 3.7.4
The organization checks media containing diagnostic and test programs for malicious code before the media are used in the information system.
Testing Performed by Compliance Auditor

Reviewed the Incident Response Plan (dated February 28, 2020) and the Incident Response Procedures (dated February 28, 2020) Interviewed the Compliance Manager regarding protections relative to protecting against and responding to identification of malicious code and determined the use of antivirus, file integrity monitoring, intrusion detection, and SIEM are always live monitored by SOC Observed evidence of at-home monitoring by SOC personnel Observed sample of tickets created from incidents and follow-up responses Observed dashboard demonstrating antivirus installation Observed SIEM reports for security and availability
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
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 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 configured to generate alerts on non-compliant machines, and logs are stored for more than 12 months
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Maintenance – Derived Security Requirements: 3.7.5
The organization requires multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.
Testing Performed by Compliance Auditor
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
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
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Maintenance – Derived Security Requirements: 3.7.6
The organization supervises the maintenance activities of maintenance personnel without required access authorization.
Testing Performed by Compliance Auditor
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

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 home-based due to COVID-19 and visitors are not being allowed into the office
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
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

MEDIA PROTECTION

Media Protection – Basic Security Requirements: 3.8.1
The organization protects (i.e., physically controls and securely stores) information system media containing CUI, both paper and digital.
Testing Performed by Compliance Auditor
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 transports by Iron Mountain are logged and tracked by Iron Mountain
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
Reviewed the Backup and Recovery Policy (dated March 31, 2020), the Data Destruction Policy (dated April 6, 2020), and the Removable Media Policy (dated April 6, 2020) and verified they address requirements for destroying removable media, digital storage, and print media Observed means for data destruction and secure storage of media prior to transferring to vendor for destruction
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Media Protection – Basic Security Requirements: 3.8.2
The organization limits access to CUI information system media to authorized users.
Testing Performed by Compliance Auditor
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 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
Reviewed the Multi-Factor Authentication Policy (dated April 6, 2020) and verified access requiring multi-factor authentication is defined Interviewed the Compliance Analyst and determined the Confluence portal is used to store system documentation and verified the system sits behind a web application firewall (WAF) and requires multi-factor authentication

Observed inventories and system documentation are available in Confluence Observed multi-factor authentication is required to access Confluence
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Media Protection – Basic Security Requirements: 3.8.3
The organization sanitizes or destroys information system media containing CUI before disposal or release for reuse.
Testing Performed by Compliance Auditor
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
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
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Media Protection – Derived Security Requirements: 3.8.4
The organization marks media with necessary CUI markings and distribution limitations.
Testing Performed by Compliance Auditor
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 corresponding classification security requirements
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Media Protection – Derived Security Requirements: 3.8.5
The organization controls access to media containing CUI and maintains accountability for media during transport outside of controlled areas.
Testing Performed by Compliance Auditor
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 transports by Iron Mountain are logged and tracked by Iron Mountain
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Media Protection – Derived Security Requirements: 3.8.6
The organization implements cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.
Testing Performed by Compliance Auditor
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 transports by Iron Mountain are logged and tracked by Iron Mountain
Reviewed the Encryption and Hashing Policy (dated March 3, 2020) and external vulnerability scans and verified the policy 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 Analyst and determined requirements for implementing encryption for all confidential data, both electronic transmissions and physical electronic media, prior to sending outside of the environment Observed evidence of backup settings including AES 256 encryption for backups Observed no other protected data owned/processed (at rest) by the organization outside of backups
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Media Protection – Derived Security Requirements: 3.8.7
The organization controls the use of removable media on information system components.
Testing Performed by Compliance Auditor

Reviewed the Backup and Recovery Policy (dated March 31, 2020), the Data Destruction Policy (dated April 6, 2020), and the Removable Media Policy (dated April 6, 2020) and verified they address requirements for handling and destroying removable media Observed means for data destruction and secure storage of media prior to transferring to vendor for destruction
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Media Protection – Derived Security Requirements: 3.8.8
The organization prohibits the use of portable storage devices when such devices have no identifiable owner.
Testing Performed by Compliance Auditor
Reviewed the Backup and Recovery Policy (dated March 31, 2020), the Data Destruction Policy (dated April 6, 2020), and the Removable Media Policy (dated April 6, 2020) and verified they address requirements for destroying removable media, digital storage, and print media Observed means for data destruction and secure storage of media prior to transferring to vendor for destruction
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Media Protection – Derived Security Requirements: 3.8.9
The organization protects the confidentiality of backup CUI at storage locations.
Testing Performed by Compliance Auditor
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
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 business operations and critical associated support functions

Observed results of recent tabletop exercise and verified continuity plans are updated based on lessons learned from the test (e.g., pandemic response)

Control Deficiencies Noted: YES ☐ NO ☒
If YES, explain the nature of the deficiency:

PERSONNEL SECURITY

Personnel Security – Basic Security Requirements: 3.9.1
The organization screens individuals prior to authorizing access to information systems containing CUI.
Testing Performed by Compliance Auditor
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 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 audit period
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 audit 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 • Nationwide Sex Offender Registry check
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Personnel Security – Basic Security Requirements: 3.9.2
The organization ensures that CUI and information systems containing CUI are protected during and after personnel actions such as terminations and transfers.
Testing Performed by Compliance Auditor

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 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 a sample of terminated/separated employees and verified evidence of removal of separated/terminated employees
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

PHYSICAL PROTECTION

Physical Protection – Basic Security Requirements: 3.10.1
The organization limits physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.
Testing Performed by Compliance Auditor
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 home-based due to COVID-19 and visitors are not being allowed into the office
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
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
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Physical Protection – Basic Security Requirements: 3.10.2
The organization protects and monitors the physical facility and supports infrastructure for those information systems.
Testing Performed by Compliance Auditor
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 home-based due to COVID-19 and visitors are not being allowed into the office
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
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
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Physical Protection – Derived Security Requirements: 3.10.3
The organization escorts visitors and monitors physical activity.
Testing Performed by Compliance Auditor
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 home-based due to COVID-19 and visitors are not being allowed into the office
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

Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Physical Protection – Derived Security Requirements: 3.10.4
The organization maintains audit logs of physical access.
Testing Performed by Compliance Auditor
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
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Physical Protection – Derived Security Requirements: 3.10.5
The organization controls and manages physical access devices.
Testing Performed by Compliance Auditor
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 home-based due to COVID-19 and visitors are not being allowed into the office
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
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Physical Protection – Derived Security Requirements: 3.10.6
The organization enforces safeguarding measures for CUI at alternate work sites (e.g., telework sites).
Testing Performed by Compliance Auditor
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
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Risk Assessment – Basic Security Requirements: 3.11.1
The organization periodically assesses the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of CUI.
Testing Performed by Compliance Auditor
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
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Risk Assessment – Derived Security Requirements: 3.11.2
The organization scans for vulnerabilities in the information system and applications periodically and when new vulnerabilities affecting the system are identified.
Testing Performed by Compliance Auditor
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 the process is consistent with policies and processes
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Risk Assessment – Derived Security Requirements: 3.11.3
The organization remediates vulnerabilities in accordance with assessments of risk.
Testing Performed by Compliance Auditor

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 the process is consistent with policies and processes
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 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 Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

Security Assessment – Basic Security Requirements: 3.12.1
The organization periodically assesses the security controls in organizational information systems to determine if the controls are effective in their application.
Testing Performed by Compliance Auditor
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 Interviewed the Compliance Manager and determined Connectria's procedures for the CAB and the Sponsor to approve new systems
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
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
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 Observed the Confluence portal used by Connectria and verified policies are maintained and accessible to all employees

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

Interviewed the Compliance Analyst and determined Connectria performs an annual review of all security policies, and KirkpatrickPrice is employed as an outside assessment firm and provides annual assessments for a variety of security control frameworks

Observed assessments performed by KirkpatrickPrice for Connectria and determined completed assessments in the past 12 months included the following:

- HITRUST
- GDPR
- PCI DSS
- FISMA
- Bill 198
- FERPA
- SOC 1
- SOC 2
- ISO 27001
- HIPAA/HITECH

Control Deficiencies Noted: YES ☐ NO ☒
If YES, explain the nature of the deficiency:

Security Assessment – Basic Security Requirements: 3.12.2

The organization develops and implements plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems.

Testing Performed by Compliance Auditor

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

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 Observed the Confluence portal used by Connectria and verified policies are maintained and accessible to all employees
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
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
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
Interviewed the Compliance Analyst and determined Connectria performs an annual review of all security policies, and KirkpatrickPrice is employed as an outside assessment firm and provides annual assessments for a variety of security control frameworks Observed assessments performed by KirkpatrickPrice for Connectria and determined completed assessments in the past 12 months included the following:

- HITRUST
- GDPR
- PCI DSS
- FISMA
- Bill 198
- FERPA
- SOC 1
- SOC 2
- ISO 27001
- HIPAA/HITECH

Control Deficiencies Noted: YES ☐ NO ☒
If YES, explain the nature of the deficiency:

Security Assessment – Basic Security Requirements: 3.12.3
The organization monitors information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.
Testing Performed by Compliance Auditor
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
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 Observed the Confluence portal used by Connectria and verified policies are maintained and accessible to all employees
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
Interviewed the Compliance Analyst and determined Connectria performs an annual review of all security policies, and KirkpatrickPrice is employed as an outside assessment firm and provides annual assessments for a variety of security control frameworks Observed assessments performed by KirkpatrickPrice for Connectria and determined completed assessments in the past 12 months included the following: • HITRUST • GDPR • PCI DSS • FISMA • Bill 198 • FERPA • SOC 1 • SOC 2 • ISO 27001 • HIPAA/HITECH
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

System and Communications Protection – Basic Security Requirements: 3.13.1
The organization monitors, controls, and protects organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
Testing Performed by Compliance Auditor
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 of devices from the 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
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 Observed evidence of backup settings, including AES 256 encryption for backups
Reviewed a list of failed logins (dated November 18, 2019), the list of successful logins (dated April 11, 2020), the PCI successful logins (April 2020), and PCI host login failures (dated January 2020) Interviewed the Compliance Analyst and determined logs are maintained in QRadar for over one year, and all network devices and server logs are relayed immediately to the SIEM (QRadar) Observed evidence of log concatenation in QRadar Observed monthly reports that are delivered to management Observed logs from a random date within the audit period were immediately accessible and thorough
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
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

System and Communications Protection – Basic Security Requirements: 3.13.2
The organization employs architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.
Testing Performed by Compliance Auditor
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 of devices from the 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
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 Interviewed the Compliance Manager and determined Connectria's procedures for the CAB and the Sponsor to approve new systems
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
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

Control Deficiencies Noted: YES ☐ NO ☒
If YES, explain the nature of the deficiency:

System and Communications Protection – Derived Security Requirements: 3.13.3
The organization separates user functionality from information system management functionality.
Testing Performed by Compliance Auditor
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
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

System and Communications Protection – Derived Security Requirements: 3.13.4
The information system prevents unauthorized and unintended information transfer via shared system resources.
Testing Performed by Compliance Auditor
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
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 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
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

System and Communications Protection – Derived Security Requirements: 3.13.5
The organization implements subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
Testing Performed by Compliance Auditor
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
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 portal tickets and verified the biannual review of the network diagram
Control Deficiencies Noted: YES ☐ NO ☒

If YES, explain the nature of the deficiency:

System and Communications Protection – Derived Security Requirements: 3.13.6
The information system denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception).
Testing Performed by Compliance Auditor
Reviewed the Firewall Configuration Policy (dated April 17, 2020) and verified it defines how firewalls are to be configured, it lists approved protocols, including rules to restrict inbound and outbound traffic, and it requires configuration exceptions to be documented and approved Interviewed the Compliance Analyst and determined exceptions to policy regarding firewall configurations and routing of traffic are documented using change control tickets and reviewed during the quarterly firewall reviews Observed exceptions requiring connections and routing outside the norm are documented and approved, as shown in the firewall change tickets and the most recent quarterly firewall reviews
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

System and Communications Protection – Derived Security Requirements: 3.13.7
The organization prevents remote devices from simultaneously establishing non-remote connections with the information system and communicating via some other connection to resources in external networks.
Testing Performed by Compliance Auditor
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 Observed evidence of backup settings, including AES 256 encryption for backups
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

Reviewed the Firewall Configuration Policy (dated April 17, 2020) and verified it defines how firewalls are to be configured, it lists approved protocols, including rules to restrict inbound and outbound traffic, and it requires configuration exceptions to be documented and approved Interviewed the Compliance Analyst and determined exceptions to policy regarding firewall configurations and routing of traffic are documented using change control tickets and reviewed during the quarterly firewall reviews Observed exceptions requiring connections and routing outside the norm are documented and approved, as shown in the firewall change tickets and the most recent quarterly firewall reviews
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

System and Communications Protection – Derived Security Requirements: 3.13.8
The information system implements cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.
Testing Performed by Compliance Auditor
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 of devices from the 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
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 Observed evidence of backup settings, including AES 256 encryption for backups
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

System and Communications Protection – Derived Security Requirements: 3.13.9
The information system terminates network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.

Testing Performed by Compliance Auditor
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 Observed Active Directory policies and verified it specifies a 15-minute screen lock timeout for Windows machines
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

System and Communications Protection – Derived Security Requirements: 3.13.10
The organization establishes and manages cryptographic keys for cryptography employed in the information system.
Testing Performed by Compliance Auditor
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
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

System and Communications Protection – Derived Security Requirements: 3.13.11
The information system employs FIPS-validated cryptography when used to protect the confidentiality of CUI.
Testing Performed by Compliance Auditor
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
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 Observed evidence of backup settings, including AES 256 encryption for backups
Reviewed a variety of policies and job descriptions 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 Interviewed the Compliance Analyst and determined regulatory, legal, and business requirements are documented and in place
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

System and Communications Protection – Derived Security Requirements: 3.13.12
The information system prohibits remote activation of collaborative computing devices and provides indication of devices in use to users present at the device.
Testing Performed by Compliance Auditor
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
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

System and Communications Protection – Derived Security Requirements: 3.13.13
The information system controls and monitors the use of mobile code.
Testing Performed by Compliance Auditor
N/A: The organization does not develop or deploy mobile code.
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

System and Communications Protection – Derived Security Requirements: 3.13.14
The information system controls and monitors the use of Voice over Internet Protocol (VoIP) technologies.
Testing Performed by Compliance Auditor
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 IP360
- Veeam
- Confluence
- Trend Antivirus
- IBM BigFix

Control Deficiencies Noted: YES ☐ NO ☒
If YES, explain the nature of the deficiency:

System and Communications Protection – Derived Security Requirements: 3.13.15
The information system protects the authenticity of communications sessions.
Testing Performed by Compliance Auditor
N/A: Connectria does not offer application development as a service to its customers.
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

System and Communications Protection – Derived Security Requirements: 3.13.16
The information system protects the confidentiality of a CUI at rest.
Testing Performed by Compliance Auditor
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 backup settings, including AES 256 encryption for backups

Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

System and Information Integrity – Basic Security Requirements: 3.14.1
The organization identifies, reports, and corrects information and information system flaws in a timely manner.
Testing Performed by Compliance Auditor
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 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
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
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

System and Information Integrity – Basic Security Requirements: 3.14.2
The organization provides protection from malicious code at appropriate locations within organizational information systems.
Testing Performed by Compliance Auditor
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 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 configured to generate alerts on non-compliant machines, and logs are stored for more than 12 months

Reviewed the Incident Response Plan (dated February 28, 2020) and the Incident Response Procedures (dated February 28, 2020)

Interviewed the Compliance Manager regarding protections relative to protecting against and responding to identification of malicious code and determined the use of antivirus, file integrity monitoring, intrusion detection, and SIEM are always live monitored by SOC

Observed evidence of at-home monitoring by SOC personnel

Observed sample subset of tickets created from incidents and follow-up responses

Observed dashboard demonstrating antivirus installation

Observed SIEM reports for security and availability

Control Deficiencies Noted: YES ☐ NO ☒
If YES, explain the nature of the deficiency:

System and Information Integrity – Basic Security Requirements: 3.14.3

The organization monitors information system security alerts and advisories and takes appropriate actions in response.

Testing Performed by Compliance Auditor

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

Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

System and Information Integrity – Derived Security Requirements: 3.14.4
The organization updates malicious code protection mechanisms when new releases are available.
Testing Performed by Compliance Auditor
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 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 configured to generate alerts on non-compliant machines, and logs are stored for more than 12 months
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

System and Information Integrity – Derived Security Requirements: 3.14.5
The organization performs periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.
Testing Performed by Compliance Auditor
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, and that antivirus, file-integrity monitoring, IDS, and SIEM are always live-monitored by the SOC 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 configured to generate alerts on non-compliant machines, and logs are stored for in excess of 12 months

Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

System and Information Integrity – Derived Security Requirements: 3.14.6
The organization monitors the information system including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.
Testing Performed by Compliance Auditor
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 of devices from the 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
Reviewed a list of failed logins (dated November 18, 2019), the list of successful logins (dated April 11, 2020), the PCI successful logins (April 2020), and PCI host login failures (dated January 2020) Interviewed the Compliance Analyst and determined logs are maintained in QRadar for over one year, and all network devices and server logs are relayed immediately to the SIEM (QRadar) Observed evidence of log concatenation in QRadar Observed monthly reports that are delivered to management Observed logs from a random date within the audit period were immediately accessible and thorough
Reviewed the Logging and Monitoring Policy (dated April 6, 2020) Interviewed the Compliance Manager and determined Connectria monitors incoming and outgoing communications will all security tools, including antivirus with HIPS, firewall rules, OSSEC QRadar, Active Directory, and SolarWinds Observed evidence of active use of multiple network, communications, SIEM, and environmental monitors and verified they include incoming and outgoing communications
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency:

System and Information Integrity – Derived Security Requirements: 3.14.7
The organization identifies unauthorized use of the information system.
Testing Performed by Compliance Auditor
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 of devices from the 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
Reviewed a list of failed logins (dated November 18, 2019), the list of successful logins (dated April 11, 2020), the PCI successful logins (April 2020), and PCI host login failures (dated January 2020) Interviewed the Compliance Analyst and determined logs are maintained in QRadar for over one year, and all network devices and server logs are relayed immediately to the SIEM (QRadar) Observed evidence of log concatenation in QRadar Observed monthly reports that are delivered to management Observed logs from a random date within the audit period were immediately accessible and thorough
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
Control Deficiencies Noted: YES ☐ NO ☒ If YES, explain the nature of the deficiency: