



# **LexisNexis Risk Solutions – Business Services**

**Report on Controls at a Service Organization  
Relevant to Security, Availability, Processing  
Integrity, Confidentiality, and Privacy  
and Tests of Operating Effectiveness**

**April 1, 2021 through March 31, 2022**

**SOC 2 Type 2**





## TABLE OF CONTENTS

<b>SECTION I – INDEPENDENT SERVICE AUDITOR’S REPORT .....</b>	<b>3</b>
Independent Service Auditor's Report.....	4
<b>SECTION II – ASSERTION OF LEXISNEXIS RISK SOLUTIONS’ BUSINESS SERVICES’ MANAGEMENT .....</b>	<b>8</b>
<b>SECTION III – LEXISNEXIS RISK SOLUTIONS’ BUSINESS SERVICES’ DESCRIPTION OF ITS BUSINESS AND PUBLIC RECORDS RESEARCH SYSTEM .....</b>	<b>10</b>
Company Overview .....	11
INFRASTRUCTURE.....	17
SOFTWARE.....	17
PEOPLE .....	18
DATA.....	18
PROCEDURES .....	19
ADDITIONAL ELEMENTS OF THE CONTROL ENVIRONMENT .....	20
Communications .....	21
Monitoring .....	23
Risk Assessment .....	24
Control Activities.....	24
Significant Changes to the System .....	29
Complementary Controls at User Organizations.....	30
Trust Services Criteria Not Relevant to the System .....	35
<b>SECTION IV - TRUST SERVICES CATEGORY, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS .....</b>	<b>36</b>
TRUST SERVICE PRINCIPLES AND RELATED CRITERION .....	37
Trust Services Principle – Common Criteria.....	37
Trust Services Principle – Availability.....	121
Trust Services Principle – Processing Integrity.....	129
Trust Services Principle – Confidentiality.....	136
Trust Services Principle – Privacy.....	139
<b>SECTION V – OTHER INFORMATION PROVIDED BY LEXISNEXIS RISK SOLUTIONS .....</b>	<b>154</b>

## SECTION I – INDEPENDENT SERVICE AUDITOR’S REPORT

## Independent Service Auditor's Report

Jeff McConnell  
Manager – Information Security  
LexisNexis Risk Solutions  
1000 Alderman Dr  
Alpharetta, GA 30005

### *Scope*

We have examined LexisNexis Risk Solutions' Business Services' ("LNRS") accompanying description of its Business and Public Records Research system found in Section III titled "LexisNexis Risk Solutions' Business Services' Description of its Business and Public Records Research System" (the "description") throughout the period April 1, 2021 to March 31, 2022 (the "period") based on the criteria for a description of a service organization's system set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (the "description criteria") and the suitability of the design and operating effectiveness of controls stated in the description throughout the period, to provide reasonable assurance that LNRS' service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy (the "applicable trust services criteria") set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

### *Complementary User Entity Controls*

The description indicates that certain complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at LNRS, to achieve LNRS' service commitments and system requirements based on the applicable trust services criteria. The description presents LNRS' controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of LNRS' controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

### *Other Information Provided by LexisNexis Risk Solutions*

The information included in Section V, "Other Information Provided by LexisNexis Risk Solutions" is presented by the Company's management to provide additional information and is not a part of the Company's description made available to user entities during the Period. Information within Section V, "Other Information Provided by LexisNexis Risk Solutions" has not been subjected to the procedures applied in the examination and accordingly, we express no opinion on it.

## *Service Organization's Responsibilities*

LNRS is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that LNRS' service commitments and system requirements were achieved. In Section II, LNRS has provided the accompanying assertion titled "Assertion of LexisNexis Risk Solutions' Business Services' Management" (the "assertion") about the description and the suitability of design and operating effectiveness of controls stated therein. LNRS is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

## *Service Auditor's Responsibilities*

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

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

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

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

## *Inherent Limitations*

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs. There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design or operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

## *Description of Tests of Controls*

The specific controls we tested, and the nature, timing, and results of our tests are listed in Section IV titled "Trust Services Category, Criteria, Related Controls, and Tests of Controls" of this report.

## *Opinion*

In our opinion, in all material respects—

- a) the description presents LNRS' Business and Public Records Research system that was designed and implemented throughout the period April 1, 2021 to March 31, 2022 in accordance with the description criteria.
- b) the controls stated in the description were suitably designed throughout the period April 1, 2021 to March 31, 2022 to provide reasonable assurance that LNRS' service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if user entities applied the complementary user entity controls assumed in the design of LNRS' controls throughout that period.
- c) the controls stated in the description operated effectively throughout the period April 1, 2021 to March 31, 2022 to provide reasonable assurance that LNRS' service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary user entity controls assumed in the design of LNRS' controls operated effectively throughout that period.

## *Restricted Use*

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of LNRS, user entities of LNRS' Business and Public Records Research system during some or all of the period April 1, 2021 to March 31, 2022, business partners of LNRS subject to risks arising from interactions with the Business and Public Records Research system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, business partners, and other parties.
- Internal control and its limitations.
- Complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.

- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

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

*Assure Professional, LLC*

Assure Professional, LLC  
Clemson, South Carolina  
August 4, 2022

## SECTION II – ASSERTION OF LEXISNEXIS RISK SOLUTIONS’ BUSINESS SERVICES’ MANAGEMENT



## Assertion of LexisNexis Risk Solutions' Business Services' Management

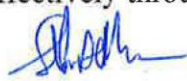
We have prepared the accompanying description of LexisNexis Risk Solutions' Business Services' ("LNRS") Business and Public Records Research system found in Section III titled "LexisNexis Risk Solutions' Business Services' Description of its Business and Public Records Research System" (the "description") throughout the period April 1, 2021 to March 31, 2022 (the "period") based on the criteria for a description of a service organization's system set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (the "description criteria").

The description is intended to provide report users with information about the Business and Public Records Research system that may be useful when assessing the risks arising from interactions with LNRS' system, particularly information about system controls that LNRS has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Processing Integrity, Confidentiality and Privacy (the "applicable trust services criteria") set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

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

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

- 1) The description presents LNRS' Business and Public Records Research system that was designed and implemented throughout the period April 1, 2021 to March 31, 2022 in accordance with the description criteria.
- 2) The controls stated in the description were suitably designed throughout the period April 1, 2021 to March 31, 2022 to provide reasonable assurance that LNRS' service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if user entities applied the complementary controls assumed in the design of LNRS' controls throughout that period.
- 3) The controls stated in the description operated effectively throughout the period April 1, 2021 to March 31, 2022 to provide reasonable assurance that LNRS' service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary user entity controls assumed in the design of LNRS' controls operated effectively throughout that period.

By:   
Title: EVP & CTO  
August 4, 2022

### **SECTION III – LEXISNEXIS RISK SOLUTIONS’ BUSINESS SERVICES’ DESCRIPTION OF ITS BUSINESS AND PUBLIC RECORDS RESEARCH SYSTEM**

## Company Overview

LexisNexis® Risk Solutions provides information designed to help clients make informed business decisions. Building on the 40-year LexisNexis® tradition as a provider and custodian of information, LNRS leverages technology, data, and scoring analytics to provide solutions for client needs. The solutions are designed to serve the multi-billion-dollar risk information industry, which includes professionals and organizations in areas such as insurance, law enforcement, government agencies, financial services firms, collection agencies, health care providers, and others.

LexisNexis® Risk Solutions is a member of the RELX Group. LexisNexis® Risk Solutions has historically been one of the fastest growing business units and a key area of strategic focus for RELX, reflecting the strong growth in demand for risk and information analytics solutions.

### About RELX Group

RELX Group is a provider of professional information and online workflow solutions in the science, medical, legal, risk information and analytics, and business sectors. RELX Group serves customers in more than 180 countries with offices in about 40 countries that create authoritative content delivered through its brands to enable customers to find the data, analysis and commentary to support their decisions. For more information, visit [www.relx.com](http://www.relx.com).

### About LexisNexis Risk Solutions Group

LexisNexis Risk Solutions Group serves customers in more than 180 countries employing over 8,000 people with offices in 24 countries around the world. Risk Solutions Group is a portfolio of brands that span multiple industries providing customers with innovative technologies, information-based analytics and decision tools and data services. Our brands provide market-specific solutions that help our customers solve problems, make better decisions, stay compliant, reduce risk and improve their operations. For further information, visit <https://risk.lexisnexis.com/group>.

### About LexisNexis Risk Solutions

LexisNexis Risk Solutions provides customers with solutions and decision tools that combine public and industry specific content with advanced technology and analytics to assist them in evaluating and predicting risk and enhancing operational efficiency.

LexisNexis Risk Solutions utilizes the power of data and advanced analytics to help our customers make better, timelier decisions. Innovative solutions enable organizations to manage risks like identity theft, fraud, money laundering and terrorism, and prevent financial crimes, and insurance and government benefit scams. Helping those without traditional credit histories obtain access to funds, assist agencies to find uncollected revenue, and research ways to improve business outcomes for healthcare companies. We also work with law enforcement to solve crimes. For further information, visit <https://risk.lexisnexis.com/>

## Products and Services Overview

### Accurint

The Accurint suite of products (i.e., Accurint for Insurance, Accurint for Collections, Accurint for HealthCare, to name a few of the derivatives), collectively referred to as “Accurint”, provides customers with information that assist in debt recovery, due diligence, fraud detection, identify verification, law enforcement, legal investigations, pre-employment screening, and tenant screening.

Accurint as an overall product is accessible via various vectors, i.e. Web based interactive, simple object access protocol/extensible markup language (SOAP/XML), and flat file based Batch. Customers, who have been properly verified and have a valid permissible purpose, utilize Accurint or a derivative of Accurint to perform queries to obtain information related to the subject for which they are searching. These searches are run against LexisNexis® Risk Solutions’ data repository using LexisNexis® Risk Solutions’ proprietary supercomputer technology platform.

### *Banko*

Banko is a processing solution now provided via the Accurint platform that automates bankruptcy notification and streamlines case management. Banko consolidates and updates bankruptcy cases daily from fifty states, the District of Columbia, Puerto Rico, Virgin Islands, and Guam, allowing users to discover, monitor, and manage changes in bankruptcy case information. It searches nationwide bankruptcy databases to identify new filings and updates to filings. Via its deceased search function, Banko assists user entities to verify deceased individuals in a given portfolio.

### Bridger

Bridger Insight solutions facilitate the real-time and batch screening of new and existing customers by combining technologies and decision making tools with comprehensive watch list screening, identity verification, extensive politically exposed persons (PEP) data, integrated news media searching, and more.

### *Watch List Screening*

Bridger Insight provides multi-faceted watch list screening and analytics utilizing a custom matching algorithm designed to help reduce false-positive rates. Watch lists currently integrated into Bridger Insight include, but are not limited to, the following:

- Office of Foreign Assets Control’s (OFAC) Specially Designated Nationals and Blocked Persons List
- United Nations Consolidated List
- Terrorist Exclusion List
- Unauthorized Banking List
- Her Majesty’s Treasury Consolidated list of financial sanctions targets (formerly known as Bank of England Consolidated List)
- Bureau of Industry and Security List

## *Identity Verification*

Bridger Insight facilitates access to other LexisNexis® Risk Solutions products and services, such as LexisNexis® Risk Solutions' Identity Verification service for verifying the identities of individuals and businesses. Like the watch list search results, identity verification results are stored within Bridger Insight for later retrieval and analysis.

LexisNexis® Risk Solutions' Identity Verification service is available through Bridger Insight at an additional cost. It is a product distinct from Bridger Insight and may require that an organization sign a separate agreement to meet additional LexisNexis® Risk Solutions credentialing requirements prior to accessing the service.

## *Politically Exposed Persons List Screening*

In order to identify and mitigate the increasing risks associated with PEPs, Bridger Insight offers access to third party providers of multi-source, multi-dimensional and multi-national PEP data. For example, Bridger Insight users can opt to access Dow Jones Public Figures and Associates (formerly Factiva® PFA) and World-Check™.

## Small Business Financial Exchange (SBFE) Data Warehouse

The SBFE Data Warehouse is a source of US small business credit information. SBFE Data Warehouse enables blind information exchange among its Members. SBFE offers risk management solutions by providing industry insight and analysis of aggregated small business financial data to its Members. The SBFE Data Warehouse application houses information allowing the following services to be provided to members.

- Small business identification data and positive and negative lending account information reported by its Members through SBFE's give-to-get exchange
- Online, real-time access to SBFE Data-driven products
- Monthly updates of each Member's portfolio data contribution statistics

## Risk Management Solutions – Evolution Platform & Legacy Risk Management Solutions Portal, AML Insight & Legacy Anti-Money Laundering, Collection Solutions, Risk Research, Real Estate Solutions, Investigative Portal

Risk Management Solutions quickly delivers information to help you authenticate the identities of both individuals and businesses. Innovative tools for authenticating identities, assessing risk and performing due diligence will help you make informed decisions utilizing intelligence and analytics to protect and grow your organization. Providing easily interpreted identity intelligence allowing businesses to more efficiently:

- Mitigate fraud
- Provide customers with satisfying onboarding experiences
- Facilitate ongoing account maintenance
- Conduct fraud and identity investigations
- Strengthen fraud recovery efforts



## Risk Defense Platform (RDP)

The LexisNexis® Risk Defense Platform is a configurable policy decisioning engine that provides single-point access to a myriad of authentication tools and industry-proven decisioning insights that keep your fraud deflection strategy ahead of the next big threat. By combining intuitive verification and authentication solutions with highly advanced analytics, including machine learning, the platform helps your business manage complex fraud and identity rules to achieve secure authentication and attain the ideal business process workflow. The platform is available via the most up to date API methods for your B2B needs.

## TrueID (via RDP and stand-alone platform)

LexisNexis® TrueID® helps organizations instantly authenticate identity documents in face-to-face or remote transactions, fight fraud and improve customer experience. TrueID Document Authentication is automated forensic analysis of ID documents including the extraction of critical personally identifiable information (PII) including, Name, Address, DOB and ID number. This is achieved using ID images acquired from ID scanners and mobile devices, sending those images for analysis either locally on a Windows PC or remotely using our web service.

## Instant ID Q&A via RDP Platform

LexisNexis® InstantID® Q&A confirms a consumer's identity in seconds and gives your financial institution an easy, real-time way to fight identity fraud at multiple points of customer contact. Simplify knowledge-based authentication (KBA) and help your business:

- Confirm identities on the spot in real time
- Expand customer touch points while mitigating fraud
- Accelerate customer onboarding
- Strengthen the customer experience
- Reduce the operational costs of authentication and improve margins

## Instant Verify via RDP Platform

Instant Verify instantly verifies personal identity data and professional credentials to allow companies to make informed decisions regarding valid identity information of applicants, customers or employees.

## Batch Solutions

LexisNexis® Batch Solutions offers powerful tools to help increase right-party contact, shorten workflow time, minimize your risk, and increase operational efficiency. Batch Solutions provides extensive, independent data sources that contain credible name, address, and phone number records. Batch Solutions leverages advanced data-linking technology to automatically search, flag, evaluate, manage, and monitor changes in consumer information.

Batch Solutions provides search products that lets clients submit large numbers of specific search requests in a text-format file to an SFTP (secure SFTP) server or Internet gateway portal to LexisNexis for processing. After the data request file is validated for the necessary data elements that are required to produce reliable search results, the data request file is processed by Batch Solutions. Clients can increase file-transfer security by sending data request files using an encrypted file format. Batch Solutions can also return your search results in an encrypted format that you can decrypt using your private encryption key.

## World Compliance

LexisNexis World Compliance Data delivers access to databases of sanctions, enforcements, PEP and adverse media. Users are able to access detailed profiles covering countries and territories throughout the globe. World Compliance monitors multiple government agency, enforcement agency and sanctioning body websites for updates to time sensitive changes to the risk landscape. Features of World Compliance include the following:

- Identify Politically Exposed Persons, their family members and associates
- Enable visibility into global adverse media profiles multiple worldwide sources
- Enable compliance workflow efficiency with data that is tailored to fit specific strategies

## Instant ID

LexisNexis InstantID is a configurable identity verification solution that allows you to verify consumer information to drive smarter decisions and keep customer acquisition in focus. InstantID combines powerful and effective identity verification, validation and fraud detection tools to instantly authenticate individuals with access to the industry's most robust database.

## Business InstantID

InstantID Business gives you the competitive advantage of next generation business verification. By combining the reach of more than 10,000 data sources with the intelligence of industry leading linking capabilities, you gain the ability to access more U.S. businesses, including hard-to-access small and new businesses; increase auto-verifications; and improve the connection between a business and a person.

## FraudPoint

FraudPoint solutions allow organizations to identify fraud incidents by detecting synthetic identity and other types of fraud resulting in significantly reduced fraud incidents and losses. LexisNexis FraudPoint minimizes administrative costs associated with inefficient and unnecessary investigation to improve your bottom line. LexisNexis FraudPoint solutions detects fraudulent applications by using advanced analytics that leverage continuously updated data facilitating comprehensive and dynamic identity and digital intelligence.

## Fraud Intelligence

LexisNexis® Fraud Intelligence is a non-FCRA solution that helps organizations mitigate new account fraud risk by using advanced analytics that leverages continuously updated LexisNexis proprietary & public record data sources. Fraud Intelligence brings together identity events and consumer application activity to arrive at a comprehensive and powerful non-FCRA fraud score that offers a more complete view of identity. Because it can identify applications that are most likely fraudulent in near real-time, it limits friction for any legitimate customers.

## OTP

LexisNexis® One Time Password is an out-of-band authentication method that provides the ability to have stronger authentication during a high risk, high value transaction with a customer. It offers a time-sensitive, unique random passcode via SMS, text, email or phone and is ideal for companies that are interested in providing a multi-factor authentication solution for their customers. No hardware (electronic fob, etc.) other than the user's existing phone or personal computer is required.

## RiskView

RiskView™ Solutions are consumer report products provided by LexisNexis® Risk Solutions Group ("LexisNexis") that are used as a factor in establishing a consumer's eligibility for credit and certain other permissible purposes set forth in the Fair Credit Reporting Act (FCRA). RiskView™ Solutions are offered as credit risk scores, as a detailed report, or as attributes to be used in internal models developed by LexisNexis customers. RiskView Scores, RiskView Report, and RiskView Attributes leverage the industry's largest collection of public records and other alternative credit data sources to provide lenders and service providers with a unique and powerful view on the creditworthiness of a consumer.

## Phone Finder

LexisNexis® Phone Finder combines authoritative phone content with the industry's largest repository of identity information to deliver relevant, rank ordered-connections between phones and identities. Phone Finder can provide a clear understanding of the associations between a phone number and an identity to help automate key account activities and support a more efficient account workflow.

## Flex ID

FlexID provides powerful data reach while supporting your need for agile verification processes that can continually adjust to serve changing marketplaces. Backed by the industry's leading consumer data repository, comprised of thousands of different sources and public records, Flex ID delivers the verification fundamentals you need to complete decisioning and conduct business.

With four configurations to choose from, Flex ID promotes confident transactions by returning the level of identity verification that matches your specific business rules.



## Boundaries of the Systems

The purpose of the system description is to delineate the boundaries of the system, which include the services outlined above and the five components described below: infrastructure, software, people, data, and procedures. The scope of this report includes the following LexisNexis Risk Solutions' facilities that support the Business and Public Records Research systems:

Facility	Function
Boca Raton, FL	Data Center Operations
Alpharetta, GA	Data Center Operations

## INFRASTRUCTURE

LNRS' information system is based on Microsoft Windows ("Windows") and Linux servers via on premises physical hardware or virtualized instances. A Windows Domain is in place to establish boundaries to the information system. The information system allows LNRS to accept data from its clients using a variety of secure methods including Secure File Transfer Protocol ("SFTP"), Transport Layer Security ("TLS") and Virtual Private Network ("VPN").

LNRS maintains a third-party agreement for redundant high speed internet access. The production networks are hosted at two separate data center facilities. LNRS procures servers and components known for reliability, serviceability, and redundancy features. Infrastructure components are implemented and configured to eliminate a single point of failure and are thoroughly tested before being installed into the production environment.

## SOFTWARE

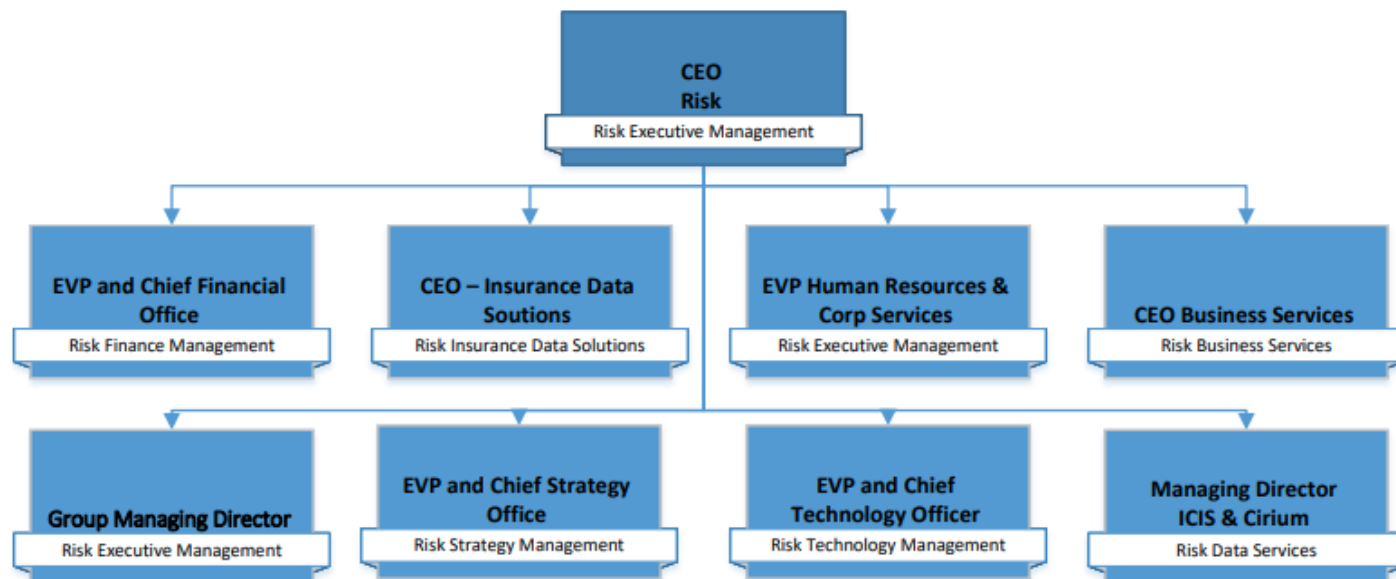
The software applications used by the system are documented in the Product and Services Overview section of this report. Logical access controls ensure system access is restricted to authorized individuals based on job functions.

Software utilized by IT to manage and support the Environment includes:

- Backup management
- Anti-Virus
- System monitoring
- Job scheduling and processing
- Network monitoring
- Security monitoring (SIEM)
- Change management
- File Integrity Checking (FIM)
- Data Loss Prevention (DLP)

## PEOPLE

The following organizational chart depicts LNRS' corporate structure:



## DATA

Data processed by the system is managed and stored in accordance with the relevant data protection policies and procedures. The data is managed, transmitted, and stored in a range of system and database technologies. Data owned, used, created, or maintained by LNRS is classified into the following categories:

- **Public:** *LNRS website and any other information that may be disclosed to anyone within or outside LNRS.*
- **General:** *Routine business information that is intended for internal use only.*
- **Restricted:** *Information that LNRS has a legal obligation to safeguard such as client data, regulated data.*
- **Confidential:** *Proprietary LNRS data, trade secrets, strategic plans, etc.*

All data flowing through LNRS infrastructure is encrypted, and access is restricted to authorized individuals requiring such access including LNRS' customer base. Such data includes Personal Identifiable Information. Logical access controls ensure access is restricted to authorized individuals based on job functions.

### **Confidentiality and Privacy**

All members of LNRS are obligated to protect confidential data in their control. Annual training is provided to all employees to address security, confidentiality and privacy. The Information Security Policy and Encryption Policy discuss the methods of protecting such information and procedures to safeguard the data during transmission. Electronic communications are more likely to leave a trail of inadvertent copies and are more likely to be seen during routine maintenance of computer systems.

## PROCEDURES

Automated and manual procedures related to the services provided include procedures by which service activities are initiated, authorized, performed, and delivered and reports or other information is prepared. Operating procedures have been documented and made available to all users who need them via the LNRS' intranet. These procedures cover the following areas:

- Data Handling/Management
- Change management
- Information security controls
- Security incident response
- Secure Software Development Lifecycle

Security is critical to the physical network, computer operating systems, and application programs. Each area offers its own set of security issues and risks. LNRS has implemented a comprehensive security program that offers a high level of protection corresponding with the value of the assets.

### *Accountability*

Individual users are responsible for ensuring that others do not access data or information from their systems. Users must take great care in protecting their usernames and passwords and this information is never to be loaned or given to other members of LNRS or outside individuals. Disclosing this information could lead to vulnerabilities of the system as well as to the data and information contained on the system.

Responsibility for guaranteeing appropriate security for data, systems, and networks is assigned to the Information Security and Information Technology Groups. The Information Security and Information Technology Groups are responsible for designing, implementing, and maintaining security protection, but management retains responsibility for ensuring compliance with this policy. In addition to management and information technology staff, the individual user is responsible for the information technology equipment and resources under his or her control.

### *Processing Integrity*

LNRS Business Services uses multiple applications to provide services to its users. Documented application security testing requirements are in place to ensure security related functionality and testing for potential security vulnerabilities and flaws is completed before they are released to production.

During the data entry process in the applications, edit/validation checks are in place to ensure the data entered is formatted correctly. They are configured to automatically perform the checks on the search data being processed. The checks are utilized by the application to help ensure personal information, and any other data required, is entered completely, accurately, and timely.

The privacy policy (<https://risk.lexisnexis.com/privacy-policy>) discusses the use of personal information and when this information is to be used for a new purpose, an opt-out option is provided for consumers. When individuals request access to their personal information, company personnel confirm the identity of the individual before they are granted any information and are required to select a permissible use.

Multiple batch job processing applications are used to monitor for processing errors. Application interfaces show the failed job with the reason behind error.

## **ADDITIONAL ELEMENTS OF THE CONTROL ENVIRONMENT**

### **The Control Environment**

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity and ethical values, competence of LNRS' people; management's philosophy and operating style; the way management assigns authority and responsibility and organizes and develops its people; and the attention and direction provided by the board of directors. LNRS has established controls which foster shared values and teamwork in pursuit of the organization's objectives.

### ***Integrity and Ethical Values***

Integrity and high ethical standards are qualities essential to LNRS' business and are viewed as fundamental standards of behavior for all employees. The effectiveness of internal controls cannot rise above the integrity and ethical values of the people, who create, administer, and monitor them. LNRS established programs and policies designed to communicate and reinforce the integrity and ethical standards of LNRS. Any employee found to have violated the ethics policy may be subject to disciplinary action, up to and including termination.

### ***Management Oversight and Organizational Structure***

LNRS' organizational structure provides the framework within which its activities for achieving entity-wide objectives are completed and analyzed. LNRS is organized in a manner which defines key areas of authority while maintaining adequate separation of duties.

### ***Roles and Responsibilities***

Everyone in LNRS has some responsibility for achieving the obligations of LNRS. Proper lines of communication are in place to discuss operational activities and risks of LNRS in a timely manner with management. LNRS' management encourages individuals and teams to use initiative in addressing issues and resolving problems.

### ***Commitment to Competence and Accountability***

LNRS defines competence as the knowledge and skills necessary to accomplish tasks that define an employee's roles and responsibilities. LNRS seeks only high-quality staff with significant experience, education, and understanding of working in a team environment. When hiring, management analyzes the knowledge and skills required to complete given tasks and confirms the individuals can complete the tasks through interviewing, reference, and background checks, as well as other investigative means.

## ***Human Resources Security***

LNRS provides Human Resources (HR) policies, procedures, and guidelines within its corporate intranet. Management updates these policies as appropriate. LNRS managers observe these policies, procedures, and guidelines as well as applicable federal and state laws, as they relate to recruitment, selection, and hiring of employees and contractors. LNRS maintains Standard Operating Procedures and expects that all employees conduct themselves in a professional and ethical manner. Additional information can be found here: <https://www.relx.com/investors/corporate-governance/code-of-ethics>.

Management collects all company property and assets (e.g., company credit cards, keys, computer, cell phone, etc.) from terminated employees. All company proprietary files are secured, and access to all electronic resources (e.g., telephone, network, computer, email, etc.) is terminated. HR maintains records on all active and terminated employees.

## **Communications**

LNRS uses a variety of methods for communication to ensure that significant events and issues are sent in a timely manner and that staff understand their role and responsibility over service and controls. These methods include the following: security awareness training, policy and process updates, departmental meetings summarizing events and changes, and the use of e-mail communications. LNRS maintains systems that manage the flow of information and facilitate communication with its customers.

Management communicates objectives related to confidentiality and privacy and any changes made to those objectives as needed.

LNRS' corporate intranet contains the policies and procedures that guide the conduct of employees and provides details of the personnel policies and benefits offered by LNRS. LNRS' Policies are reviewed at minimum on an annual basis, with revisions and updates released as needed. Employees complete training on an annual basis to review LNRS' policies and procedures.

The communication system between senior management and LNRS staff includes the use of the office e-mail system, written memos when appropriate, and ad-hoc meetings. Periodic department meetings between each manager and their staff are also held to discuss new company policies and procedures and other business issues. Staff and training meetings are utilized to inform staff of new policy and technology updates. Communication is encouraged at all levels to promote the operating efficiency of LNRS.

## ***Policies***

LNRS maintains a suite of comprehensive policies designed to provide both management's stated direction (policy) and staff working practices (procedures). These documents are posted on LNRS' intranet and are available to all employees.

Policies address the reasons for security; the rules and procedures required to achieve security; and the personnel and roles who work to enforce the security policies.

The accompanying table lists an example of the policy documents that have been adopted by LNRS.

Policies	Description
Electronic Workplace Policy Bring Your Own Device (BYOD) Policy Mobile Device Security Social Media Policy	Policies governing how computing resources may be used
Information Value Classification Policy Data Destruction Standards Record Retention Schedule Record Management Policy Compliance Management System Policy Confidentiality & Non-Disclosure Agreement	Policies related to the creation, exposure, and disposal of data, both corporate and client
Information Security Policy Computer and Network Security Policy Secure System Installation Procedures User Access Control Procedures	Policies that cover the security of network attached resources and the network infrastructure that serves these resources
Data Backup Policy Technical Resilience Program Processes and Procedures Change Management Standards Secure Software Development Lifecycle Standards Incident Response and Notification Policy Risk Assessment Procedures 3 <sup>rd</sup> Parties Security Policy Vulnerability Management Standards	Policies, rules, and procedures covering actions that affect the ongoing maintenance and availability of a secure infrastructure.
Physical Security Program Remote Access Policy Encryption Policies Asset Management Policy	Policies covering the security of Information Technology assets



## ***Published Job Descriptions***

Job descriptions aid in establishing hiring criteria, orienting new employees to their jobs, identifying the requirements of each position, setting standards for employee performance evaluations, and establishing a basis for making reasonable accommodations for individuals with disabilities. LNRS makes every effort to create and maintain accurate job descriptions for all positions within the organization. Each description at a minimum includes the job title and the duties for the position. Additional requirements are listed depending on the position. All employees will be expected to help ensure that their job descriptions are accurate and current, reflecting the work being done.

## ***Operating Procedure Manuals***

Procedure manuals enhance consistency in operating procedures and provide a reference to employees in the conduct of their daily responsibilities. The manuals maintained and updated include:

- LNRS user reference manuals, which provide the primary resources to company staff for operational software use.
- Technical manuals, ranging in subject from computer operations guides to process manuals, which serve as a valuable resource to many different positions within LNRS.

## ***Training***

LNRS has implemented various methods of communication to help ensure that employees understand their individual roles and responsibilities over user data and controls, and that significant events are communicated in a timely manner. LNRS is committed to training as an essential part of the success of each employee. IT management conducts security training programs for all employees. Newly hired employees undergo security awareness training to introduce the employee to confidentiality and privacy requirements. In addition, managers oversee the review and acknowledgments of LNRS' policies.

## ***Monitoring***

LNRS management performs monitoring activities as part of normal business operations to assess the quality of the internal control environment. Management performs regular reviews of tasks assigned to their teams. Monitoring activities are used to initiate corrective action through team meetings, client conference calls, and informal notifications. Corrective actions are taken as required to correct deviations from company policy and procedures. Tasks that are not addressed in a timely manner are escalated and resolved.

## ***Performance Evaluations***

The primary objective of a performance evaluation is to measure the performance of an individual against the objective standards established for a specific position. Consequently, the main purpose of the LNRS performance evaluation program is to provide an equitable method to assess an employee's job performance, discuss performance and actions to improve job performance, identify an employee's development needs, and provide for salary administration.

LNRS employees undergo performance reviews to identify both strengths and areas in need of improvement. All employees, regardless of classification or length of service, are expected to meet and maintain company standards for job performance and behavior. Performance goals are determined for the next year. Reviews may also be conducted in the event of a promotion or change in duties and responsibilities.

## **Risk Assessment**

Every entity faces a variety of risks from external and internal sources that must be assessed. A precondition to risk assessment is establishment of objectives, linked at different levels and internally consistent. Risk assessment is the identification and analysis of relevant risks to the achievement of LNRS objectives and forming a basis for determining how the risks should be managed. Because economic, industry, regulatory and operating conditions will continue to change, mechanisms are needed to identify and deal with the special risks associated with change.

Management identifies risks that threaten client commitments by performing a formal risk assessment at least annually. The risk assessment includes the analysis of fraud, threats and vulnerabilities, probabilities of occurrence, potential business impacts, and associated mitigation plans. Management holds risk management meetings throughout the year so that it can react swiftly to address emerging risks. Risk mitigation strategies include prevention and elimination through the implementation of internal controls and transference of risk through insurance policies.

LNRS maintains insurance coverage to transfer certain identified risks. LNRS maintains a general liability and umbrella policy to protect against unforeseen events. Additional insurance policies may be acquired as needed to satisfy certain contractual obligations.

## **Control Activities**

### ***Security Management***

LNRS implements Security practices to help protect physical access to data and systems and to limit access to authorized personnel. LNRS has instituted Security Awareness Training and the LNRS workforce is trained on security expectations.

Additionally, LNRS meets periodically to discuss current security issues and concerns for its services.

### **Information Security**

The information security program provides reasonable protection against unauthorized access, disclosure, modification, or destruction, as well as to assure the availability, integrity, usability, authenticity, and confidentiality of information. This applies to all systems that manage or store data.

The Information Security Policy serves to establish the minimum information security practices for LNRS Sensitive Data computer resources and associated communication networks. Furthermore, the policy is intended to give direction on Sensitive Data security practices that are designed to ensure confidentiality, integrity, and availability of corporate data. Sensitive Data includes but is not limited to Personal Information, Internal Documents, and documents classified as Confidential. Access to systems containing such information is restricted on a need to know and business need basis. Multiple security domains are in place to segregate environments that require a higher level of security and access is restricted to individuals with a business need.

### **Logical Access**

Access to resources and data are granted to individuals based on their job responsibilities. New user accounts are established only upon receipt of properly authorized requests. The Information Assurance and Data Protection (IADP) team acts as the security administrators and is responsible for ensuring adherence to the security policy which addresses logical access control procedures.



Individual access capabilities are removed by IT or data owners upon the notification of termination of employment, change of responsibilities, or termination of a contract with a client that uses the system. System security access levels are periodically reviewed by management, IT and data owners to ensure individual access rights are appropriate based on job information.

### Password Settings

LNRS follows a structured user and password management procedures that is documented within the LNRS User Access Control Procedures document. LNRS utilizes an initial strong complex password for the user which must be changed at first login. All user accounts password is set to expire after a set number of days. Password complexity, history, maximum password age, minimum password age and minimum password lengths are enabled and established.

## ***Computer Operations & Data Communications***

LNRS utilizes several network security technologies to protect and defend Internet-accessible systems.

### Firewalls

Redundant firewalls protecting the intranet from the public network are implemented, configured, and managed by the LNRS administration staff. Firewalls utilized access rules to grant or deny access to internal resources.

### Demilitarized Zone (DMZ)

Network computers exposed to the Internet can subject the entire network to detrimental attacks. This can lead to compromised data, viruses, and other types of malicious acts that could damage LNRS' credibility and operations.

A Demilitarized Zone has been established to isolate LNRS' computers from the Internet. A Demilitarized Zone is a small network of computers exposed to the external world (Internet). Identifiable security incidents occurring on the DMZ computers are evaluated, and steps would be taken to prevent future breaches of the DMZ.

### Data Transmission and Encryption

Data in motion is encrypted using TLS level encryption. Data can be accessed remotely using a virtual private network with multi-factor authentication. A VPN is used to provide secure, encrypted communication between a network and a remote host or other remote networks over the public Internet. VPNs allow the establishment of an encrypted tunnel that protects the flow of network traffic from eavesdroppers. Instead of using a dedicated, real world connection such as a leased line, a VPN uses virtual connections routed through the Internet from the private network to the remote site or employee.

### Private Data

The LNRS privacy policy is available to data subjects and when receiving private, or sensitive data, LNRS obtains consent in compliance with applicable regulations. LNRS reviews the privacy policy annually and any changes are communicated to data subjects timely. As new services are developed, LNRS has a process to identify when new private data is required so that consent can be obtained in a timely manner. LNRS has several processes in place to validate the private information received from data subjects is accurate and complete. Private data is only retained for as long as needed to provide services to its clients and for LNRS to meet its legal and regulatory obligations.

## **Secure Storage, Media, Data and Document Destruction**

LNRS has established Data Destruction Standards to direct how and when to destroy data. All computer systems, electronic devices, and electronic media are properly cleaned of sensitive data and software before being transferred outside of the corporate office either as surplus property, donation, or as trash.

Non-rewriteable media are sanitized by physical destruction. Re-writable media must be destroyed using methods so that information is not recoverable in either the corporate or cloud environment using deletion or overwrite protocol.

LNRS personnel are required to shred paper documents and delete electronic documents classified as confidential or restricted.

## **Incident Response**

Incident management is not only a necessary practice for internal LNRS operations, but it is also a key component fulfilling LNRS' obligations to its Customers regarding the service offerings. Effective incident management can ensure LNRS operations, reduce downtime, and increase customer confidence in LNRS' ability to service its outsourcing needs.

Procedures direct that any incidents should be reported to the Incident Response Team utilizing one of the published communication methods. The IRT is responsible for establishing all security incident response and escalation procedures including the documentation and the distribution to ensure timely and effective handling of all situations. Since not all potential incident types can be listed a standardized process is in place to handle incidents or exceptions.

An incident can be defined as any event that adversely impacts the normal operations of LNRS information systems and/or jeopardizes the security, confidentiality, operations, integrity, or availability of LNRS information assets, systems, databases, applications, products, or personal information files.

## **Vulnerability and Patch Management**

LNRS manages the installation of operating system and supporting software, as well as the deployment of necessary security patches and operating system services packs. Vulnerability patches require timely adoption to maintain the operational availability, confidentiality, and processing integrity of computer systems, networks, and applications.

All critical systems are patched to the most recently released, appropriate software patches to protect against exploitation and compromise of data by malicious individuals and malicious software.

LNRS employs vulnerability reporting systems and subscribes to security bulletins to identify the most recent software patch versions and software to identify the production equipment that is out of compliance and requires updates. Other applications are patched as patches are released by the vendor and scheduled in accordance with the LNRS Patch Management Policy.

### Patch Deployment

LNRS' IT manager reviews each patch carefully to determine if it is necessary to deploy it within the production environment. If the IT manager decides that the patch is necessary and should be deployed, the patch is tested. Once the patch has been thoroughly tested, it is approved for deployment in the production environment.

### Malicious Code Management

Anti-virus tools are used to protect servers, workstations, and where applicable network devices. A comprehensive virus management solution works to prevent virus infections and automates the virus definition updating process. The installed anti-virus application scans production servers and workstations for viruses and infected files. Infected files are cleaned. Files which cannot be cleaned are quarantined. Quarantined files are removed and/or virus removal tools are utilized to clean the impacted systems.

LNRS also utilizes automated file integrity monitoring (FIM) software to validate the file integrity of the operating system to ensure there is no unauthorized modification to critical system files.

### **Backup and Disaster recovery**

LNRS has implemented various backup methods as part of its production operations. Automated software is utilized to perform the backups of production servers. System backups are conducted, and data replication processes are implemented to enable restoration of systems in accordance with established recovery point objectives. Backups are performed daily. The backup repositories require authorized access through the user of user credentials.

### Backup Testing

Restores from backups are performed as an ongoing component of normal business operations. Servers can be restored from images to deploy new server instances or for development and testing purposes.

### Monitoring

The backup system logs the results back to the enterprise monitoring and ticketing application on the cloud administration server. Daily monitoring is performed by the administrator to ensure that the backups completed successfully.

### Recovery

LNRS has a documented recovery plan in place, and it is reviewed. LNRS maintains redundant/failover data centers so that restoration of data and services is seamless if there is an incident. Periodically, the plan is tested through a series of exercises from tabletop to complete failover events. Any issues resulting from these tests are incorporated into the plan and updates are made accordingly.

### **Network Monitoring**

Monitoring policies and procedures are utilized for addressing issues relating to outages of critical services or other issues needing immediate action. These procedures vary based on the defined severity level of the problem. LNRS engineers use several monitoring tools to identify and provide alerts.

LNRS utilizes a suite of monitoring tools to provide proactive incident identification and response services. LNRS' Information Technology team regularly monitors the network. Overall health and capacity are monitored to ensure the system will meet clients' needs. The monitoring applications generate alerts when predefined thresholds are exceeded on the monitored devices. Information Technology monitors security access violations, including server logs and reports.

## **System Maintenance and Change Management**

LNRS follows a structured change management process that is documented within the LNRS Change Management Procedures.

### Infrastructure Change Management

All changes to the production infrastructure and data environments follow the *Change Management Standards*. The *Change Management Standards* include:

- Documenting the change request in a ticket with the relevant information.
- Submitting the change request to the individuals identified as Change Approvers for groups that may be affected by the proposed change.
- Thorough testing is performed to verify that the security of the environment is not reduced by implementing a change, and testing must validate that all existing security controls remain in place, or are replaced with equally strong controls, or are strengthened after any change to the environment.
- Final change approvals are documented in the change ticket prior to implementation of the change.

### Secure Software Development Life Cycle ("SSDLC")

LNRS follows a controlled approach to developing, testing, approving, and building each release of the system that is designed to ensure continued quality of the released product before it is available to the client base.

This documented development policy is referred to as the Secure Software Development Lifecycle Standards.

The Secure Software Development Lifecycle Standards outline the phases that all development efforts go through, including but not limited to:

- Concept and Planning
- Requirements and UI
- Design and Development
- Coding
- Certification and Testing
- Prod and Release

A software application is used to manage the application development tickets utilizing a defined process. The Development Team utilizes defined code review in the development of applications. Version control software is also used to maintain current and historical versions of files such as source code, web pages, and documentation.

LNRS maintains segregated access and permissions to the different environments. Only properly tested and properly authorized changes to the production environment are deployed.

## **Data Center**

### Environment Security – Data Center

The environmental systems at the data center are managed and maintained by the personnel at the facility. Several controls are in place to protect against environmental threats. Features of the data center include:

- **Backup Power** – The facility utilizes a redundant source of UPS systems. In the event of an electrical failure, the battery-powered electrical supply system provides temporary power. In the event of extended power outages, a generator is located on site and is dedicated to the data center. An automatic transfer switch controls the power load when switching between commercial and auxiliary power.
- **Data Center Cooling** – The temperature of the facility is controlled by an air conditioning unit. A redundant HVAC system is utilized in the event of a failure to the primary unit. The server cabinets in the data center are designed for optimal air flow. Additionally, the temperature and humidity levels are monitored against predefined thresholds.
- **Data Center Fire Detection and Suppression** – The data center is equipped with VESDA (Very Early Smoke Detection Apparatus), conventional fire detection and fire suppression systems. The local administrators are the main component of the fire prevention system that detects heat, smoke, and alerts. A third-party specialist monitoring agreement is in place for detection of fire.

### Physical Access - Data Center

Data center personnel are on duty during normal business hours. Only authorized personnel have access to the data center facility and are restricted through the use of a badge-based access control system. Access to the restricted data center areas is controlled by multi-factor authentication including biometric recognition access control systems. Non-business hour building access is restricted to authorized users and requires a proximity access card which is managed and maintained by management.

Closed circuit video surveillance has been installed at all entrance point on the interior and exterior of the building and is monitored by authorized data center personnel. Motion detectors and unauthorized access are monitored.

Software is utilized to manage the surveillance system which allows for real time and ad hoc review of recordings. The system can be viewed by authorized staff both on-site and remotely via a web browser.

## **Significant Changes to the System**

No significant events or conditions were noted by management during the audit examination period.

## **Trust Services Categories and Related Control Activities**

The Trust Services Categories and related control activities are included in Section IV of this report and have been removed from the description to eliminate redundancy. The control activities listed in Section IV are, nevertheless, an integral part of LNRS' description of controls.

The description of the service auditor's tests of operating effectiveness and the results of those tests are also presented in Section IV, adjacent to the service organization's description of controls. The description of the tests of operating effectiveness and the results of those tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

## Complementary Controls at User Organizations

LNRS' applications are designed with the assumption that certain controls would be implemented by user organizations. In certain situations, the application of specific controls at the user organization is necessary to achieve control objectives included in this report.

This section describes additional controls that should be in operation at user organizations to complement the controls at LNRS. User auditors should consider whether the following controls have been placed in operation at the user organizations:

### *Security (Common Criteria)*

ID	Criteria
CC 2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.
	<ul style="list-style-type: none"><li>User organizations are responsible for controls to input complete and accurate information and comply with the operating instructions of LNRS' applications.</li></ul>
CC 2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
	<ul style="list-style-type: none"><li>User organizations are responsible for controls to comply with the operating instructions of LNRS' products and applications.</li></ul>
CC 2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.
	<ul style="list-style-type: none"><li>User organizations are responsible for controls to communicate with LNRS regarding failures, incidents, concerns, and other matters when complying with the operating instructions of LNRS' products and applications.</li></ul>
CC 3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.
	<ul style="list-style-type: none"><li>User organizations are responsible for informing LNRS of any regulatory issues that may affect the services provided by LNRS.</li></ul>
CC 3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives
	<ul style="list-style-type: none"><li>User organizations are responsible for risks related to the use of IT and access to information when granting access to the services provided by LNRS.</li></ul>
CC 3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.
	<ul style="list-style-type: none"><li>User organizations are responsible for controls to comply with the operating instructions of LNRS' products and applications.</li><li>User organizations are responsible for controls to notify LNRS in a timely manner when changes are made to technical, billing, or administrative contact information.</li></ul>



*Security (Common Criteria, Continued)*

ID	Criteria (Continued)
CC 6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.
	<ul style="list-style-type: none"> <li>• User organizations are responsible for controls to provide reasonable assurance that output reports are reviewed by appropriate individuals for completeness and accuracy.</li> <li>• User organizations are responsible for system sign-on controls and procedures for the selection and printing of available reports at their respective locations.</li> <li>• User organizations are responsible for controls to ensure that user organizations adopt strong operating system and application password management procedures, including using passwords that cannot be easily compromised and require to change on a regular basis.</li> <li>• User organizations are responsible for controls to ensure the confidentiality of any user IDs and passwords assigned.</li> </ul>
CC 6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users, whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
	<ul style="list-style-type: none"> <li>• User organizations are responsible for system sign-on controls and procedures for the selection and printing of available reports at their respective locations.</li> <li>• User organizations are responsible for controls to ensure that user organizations adopt strong operating system and application password management procedures, including using passwords that cannot be easily compromised and require to change on a regular basis.</li> <li>• User organizations are responsible for controls to ensure the confidentiality of any user IDs and passwords assigned.</li> </ul>
CC 6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.
	<ul style="list-style-type: none"> <li>• User organizations are responsible for controls to notify LNRS in a timely manner when changes are made to technical, billing, or administrative contact information.</li> </ul>
CC 6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.
	<ul style="list-style-type: none"> <li>• User organizations are responsible for procedures to define developing, maintaining, and testing their own business continuity plans ("BCP").</li> </ul>

## Security (Common Criteria, Continued)

ID	Criteria (Continued)
CC 6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.
	<ul style="list-style-type: none"> <li>User organizations are responsible for controls to provide reasonable assurance of the transmission and receipt of information not provided by LNRS.</li> </ul>
CC 7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.
	<ul style="list-style-type: none"> <li>User organizations are responsible for controls to immediately notify LNRS of any actual or suspected information security breaches, including compromised user accounts.</li> </ul>
CC 7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.
	<ul style="list-style-type: none"> <li>User organizations are responsible for controls to immediately notify LNRS of any actual or suspected information security breaches, including compromised user accounts.</li> </ul>

## Availability

ID	Criteria
A 1.2	The entity authorizes, designs, develops, or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.
	<ul style="list-style-type: none"> <li>User organizations are responsible for controls to provide reasonable assurance that the customer has procedures in place for developing, maintaining, and testing their own business continuity plans ("BCP").</li> <li>User organizations are responsible for approving the telecommunications infrastructure controls between itself and LNRS.</li> </ul>
A 1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.
	<ul style="list-style-type: none"> <li>User organizations are responsible for controls to provide reasonable assurance that the customer has procedures in place for developing, maintaining, and testing their own business continuity plans ("BCP").</li> </ul>



## Processing Integrity

ID	Criteria
PI 1.2	The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives.
	<ul style="list-style-type: none"><li>• User organizations are responsible for controls to provide reasonable assurance that erroneous input data are corrected and resubmitted.</li></ul>
PI 1.3	The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity's objectives.
	<ul style="list-style-type: none"><li>• User organizations are responsible for controls for approving the telecommunications infrastructure between itself and LNRS.</li><li>• User organizations are responsible for controls to provide reasonable assurance those transactions are appropriately authorized, complete, and accurate.</li></ul>
PI 1.4	The entity implements policies and procedures to make available or deliver output completely, accurately, and timely in accordance with specifications to meet the entity's objectives.
	<ul style="list-style-type: none"><li>• User organizations are responsible for controls to provide reasonable assurance that changes to processing options (parameters) are appropriately authorized, approved, and implemented.</li><li>• User organizations are responsible for controls to provide reasonable assurance that output reports are reviewed by appropriate individuals for completeness and accuracy.</li></ul>

ID	Criteria
P 6.5	The entity obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's objectives related to privacy.
	<ul style="list-style-type: none"> <li>User organizations are responsible for controls to immediately notify LNRS of any actual or suspected information security breaches, including compromised user accounts.</li> </ul>
P 6.6	The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.
	<ul style="list-style-type: none"> <li>User organizations are responsible for informing LNRS of any regulatory issues that may affect the services provided by LNRS.</li> <li>User organizations are responsible for controls for user organizations to ensure compliance with contractual requirements.</li> <li>User organizations are responsible for controls for the supervision, management, and control of the use of LNRS' applications by its personnel.</li> <li>User organizations are responsible for controls to maintain their own systems of recordkeeping.</li> <li>User organizations are responsible for controls to dictate the use of encryption.</li> </ul>

The list of user organization control considerations presented above and those presented with certain specified control objectives do not represent a comprehensive set of all the controls that should be employed by user organizations. Other controls may be required at user organizations. Processing of information for customers by LNRS covers only a portion of the overall internal control structure of each customer. LNRS' products and services were not designed to be the only control component in the internal control environment. Additional control procedures are required to be implemented at the customer level. It is not feasible for all the control objectives relating to the processing of transactions to be completely achieved by LNRS. Therefore, each customer's system of internal controls must be evaluated in conjunction with the internal control structure described in this report.

## Trust Services Criteria Not Relevant to the System

ID	Criteria	Reason for Exclusion
P1.1	The entity provides notice to data subjects about its privacy practices to meet the entity's privacy commitments and system requirements. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's privacy commitments and system requirements	LNRS does not engage directly with consumers. The information is obtained legally through both public and private sources. A review by LNRS' legal team ensures compliance with all laws and regulations. As such, LNRS cannot provide notice to data subjects. Data subjects can access the privacy policy located on LNRS' website for detailed instructions on how to obtain the information in LNRS' possession and their rights.
P2.1	The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.	LNRS does not engage directly with consumers. The information is obtained legally through both public and private sources. A review by LNRS' legal team ensures compliance with all laws and regulations. As such, LNRS cannot provide choices to data subjects. Data subjects can access the privacy policy located on LNRS' website for detailed instructions on how to obtain the information in LNRS' possession and their rights.
P3.2	For information requiring explicit consent, the entity communicates the need for such consent, as well as the consequences of a failure to provide consent for the request for personal information and obtains the consent prior to the collection of the information consistent with the entity's privacy commitments and system requirements.	LNRS does not engage directly with consumers. The information is obtained legally through both public and private sources. A review by LNRS' legal team ensures compliance with all laws and regulations. As such, LNRS cannot provide notice to data subjects. Data subjects can access on the privacy policy located on LNRS' website for detailed instructions on how to obtain the information in LNRS' possession and their rights.
P6.1	The entity discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.	LNRS does not get consent from individuals. Aggregate data originates from sources or in specific products like Payment Protection, and PHI is obtained from the Covered Entity.

## SECTION IV - TRUST SERVICES CATEGORY, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS

## TRUST SERVICE PRINCIPLES AND RELATED CRITERION

### Trust Services Principle – Common Criteria

*Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC1.0	Common Criteria Related to Control Environment		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC1.1	The entity demonstrates a commitment to integrity and ethical values as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	Employees are required to acknowledge LNRS' Code of Conduct that guides employees on LNRS' principles and conduct.	Inspected the Code of Conduct acknowledgment as included in the signed offer letter for the sampled new hires to determine that documentation was in place to guide employees on the organization's ethical principles and conduct.	No Exceptions Noted
	A Board of Directors is in place to provide governance on LNRS' directions and operations.	Inspected the Board of Directors as listed on the public website to determine that an independent Board of Directors is in place to provide governance on LNRS' directions and operations.	No Exceptions Noted
	Employee evaluations are performed on a regular basis against individual objectives derived from LNRS' goals, established standards, and specific job responsibilities.	Inspected the evaluations for the sample selected active employees to determine that employee evaluations were performed on a regular basis against individual objectives derived from the organization's goals, established standards, and specific job responsibilities.	No Exceptions Noted
	There are formal discipline policies for employees who are suspected of rule infractions or violations of LNRS' policies.	Inspected the disciplinary process documents to determine that there was a formal policy for employees who were suspected of rule infractions or violations of LNRS' policies.	No Exceptions Noted

## Trust Services Principle – Common Criteria (Continued)

*Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC1.0	Common Criteria Related to Control Environment (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	A Board of Directors is in place to provide governance on LNRS' directions and operations.	Inspected the Board of Directors as listed on the public website to determine that an independent Board of Directors is in place to provide governance on LNRS' directions and operations.	No Exceptions Noted

**Trust Services Principle – Common Criteria (Continued)***Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC1.0 Common Criteria Related to Control Environment (Continued)			
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	Organizational charts are in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel.	Inspected the organizational chart to determine that documentation was in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel.	No Exceptions Noted
	LNRS is segregated into separate and distinct functional areas for the purposes of the management and processing of customer information.	Inspected the organizational chart to determine that the organization was segregated into separate, logical, and distinct functional areas for the purpose of management and processing of customer information.	No Exceptions Noted
	LNRS has documented job descriptions that describe the roles and responsibilities of the position.	Inspected the job descriptions for the sampled roles to determine they were in place and described the roles and responsibilities of the position.	No Exceptions Noted
	Security Planning and Maintenance responsibilities have been delegated.	Inspected the security planning delegation and conducted a corroborative inquiry of management to determine that responsibility for Security Planning and Maintenance had been delegated.	No Exceptions Noted

## Trust Services Principle – Common Criteria (Continued)

*Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC1.0	Common Criteria Related to Control Environment (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	Responsibility for implementing, reviewing and approving LNRS' security policies has been delegated to appropriate teams within the organization.	Inspected the Information Security teams organizational charts to determine that responsibility for IT functions had been delegated to appropriate teams within the organization.	No Exceptions Noted
	LNRS has designated a Privacy Officer who is responsible for HIPAA privacy matters in LNRS.	Inspected the Chief Privacy Officer job description to determine that a Privacy Officer was defined.	No Exceptions Noted



**Trust Services Principle – Common Criteria (Continued)***Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC1.0	Common Criteria Related to Control Environment (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	LNRS provides employees access to an internal intranet, which contains policies that identify and describe management's philosophy, operating style, employee obligations and provides HR policy guidance to employees.	Inspected the available policies and procedures on LNRS' intranet to determine that management's philosophy and operating style were documented and communicated to employees via the employee handbook and that it provided HR policy guidance to employees.	No Exceptions Noted
	Management has documented its human resource policies and practices.	Inspected the HR policy documents to determine that management documented its human resource policies and practices were documented and in place.	No Exceptions Noted
	Policies are in place to provide guidance in evaluating the experience and training of candidates for employment before they assume the responsibilities of their position.	Inspected the screening, interviewing, and hiring process documents to determine that a policies are in place to provide guidance in evaluating the experience and training of candidates for employment before they assume the responsibilities of their position.	No Exceptions Noted
	During the hiring process, a background check is performed on potential employees.	Inspected the background checks for the sampled new hire employees to determine that during the hiring process, a background check was performed on employees during the hiring or onboarding process.	No Exceptions Noted

## Trust Services Principle – Common Criteria (Continued)

*Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC1.0	Common Criteria Related to Control Environment (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	Employee evaluations are performed on a regular basis against individual objectives derived from LNRS' goals, established standards, and specific job responsibilities.	Inspected the evaluations for the sample selected active employees to determine that employee evaluations were performed on a regular basis against individual objectives derived from the organization's goals, established standards, and specific job responsibilities.	No Exceptions Noted
	Full-time employees are given Security Awareness training during their new hire orientation and are then updated on an annual basis.	Inspected the security awareness training logs for the sampled new hires and active employees to determine that staff were given Security Awareness training during their new hire orientation and then updated on an annual basis.	No Exceptions Noted
	Contractors working on LNRS' systems are required to undergo security awareness training on a periodic basis.	Inspected the security training logs for the sampled contracted employees to determine that contractors working on LNRS' systems are required to undergo security awareness training on a periodic basis.	No Exceptions Noted

**Trust Services Principle – Common Criteria (Continued)***Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC1.0	Common Criteria Related to Control Environment (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	LNRS provides employees access to an internal intranet, which contains policies that identify and describe management's philosophy, operating style, employee obligations and provides HR policy guidance to employees.	Inspected the available policies and procedures on LNRS' intranet to determine that management's philosophy and operating style were documented and communicated to employees via the employee handbook and that it provided HR policy guidance to employees.	No Exceptions Noted
	LNRS considers fraud when completing its risk assessment.	Inspected the fraud considerations in the risk assessment to determine that LNRS included fraud within their risk assessment.	No Exceptions Noted
	Policies are in place that guides staff on the appropriate use of LNRS' computers, information systems, and adherence to security policies.	Inspected the Electronic Workplace Policy, the Mobile Device Security Procedures, and the Restricted Information Products and Product Data Policy to determine that an Acceptable Use Policy was in place that guides staff on the appropriate use of LNRS' computers, information systems, and adherence to security policies.	No Exceptions Noted
	Employees must sign a confidentiality agreement as acknowledgment not to disclose proprietary or confidential information.	Inspected the confidentiality agreements for the sample selected new hire employees to determine that employees were required to sign the agreement not to disclose proprietary or confidential information.	No Exceptions Noted

**Trust Services Principle – Common Criteria (Continued)***Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC1.0	Common Criteria Related to Control Environment (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	Employee evaluations are performed on a regular basis against individual objectives derived from LNRS' goals, established standards, and specific job responsibilities.	Inspected the evaluations for the sample selected active employees to determine that employee evaluations were performed on a regular basis against individual objectives derived from the organization's goals, established standards, and specific job responsibilities.	No Exceptions Noted
	There are formal discipline policies for employees who are suspected of rule infractions or violations of LNRS' policies.	Inspected the disciplinary process documents to determine that there was a formal policy for employees who were suspected of rule infractions or violations of LNRS' policies.	No Exceptions Noted
	Employees are monitored for compliance with LNRS' Code of Conduct.	Inspected the Code of Conduct acknowledgments and employee evaluations for the sampled new hire and active employees, respectively, to determine if procedures were in place to monitor compliance with LNRS' Code of Conduct.	No Exceptions Noted
	Employees are aware of the limits existing for their use of the organization's information and assets associated with information processing facilities and resources; and they are responsible for their use of any information resource and of any use carried out under their responsibility.	Inspected the Internal Use of LexisNexis Restricted Information Products and Product Data Policy to determine a policy was in place to provide guidance on the use of the organization's information and assets associated with information processing facilities and resources.	No Exceptions Noted

## Trust Services Principle – Common Criteria (Continued)

*Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC2.0 Common Criteria Related to Communication and Information			
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	Internal auditing of LNRS' processes is performed periodically.	Inspected the internal auditing schedules to determine that periodic internal auditing was performed.	No Exceptions Noted
	LNRS has documented standard operating procedures to communicate the responsibilities and requirements in the operation of the system.	Inspected the example SOP documents and conducted corroborative inquiry of management to determine that standard operating procedures were documented and in place.	No Exceptions Noted
	The Information Security Policy is reviewed annually, updated, and approved by management to remain current.	Inspected the Information Security Policy review date to determine that LNRS policies were reviewed, updated, and approved by management within the previous twelve months.	No Exceptions Noted
	A monitoring application is utilized to monitor network devices and critical systems.	Inspected the monitoring tools dashboards and available reports to determine that the organization utilized monitoring applications to measure production systems utilization and availability.	No Exceptions Noted
	Status reports from the enterprise monitoring applications can be generated for adhoc review.	Inspected the monitoring tool dashboards and filtering functionality to determine that status reports were available for adhoc review.	No Exceptions Noted
	LNRS has a Security Incident Response Policy and Procedures in place to provide policy guidance and establish responsibilities for responding to and reporting security breaches.	Inspected the Data Security Incident Response Overview and Incident Response and Notification Policy to determine that LNRS had a Security Incident Response Policy and Procedures in place to provide policy guidance for responding to and reporting security breaches.	No Exceptions Noted

**Trust Services Principle – Common Criteria (Continued)***Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC2.0 Common Criteria Related to Communication and Information			
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	Network security event logging is configured to log specific events on the network domain.	Inspected the security event logging configuration and conducted a corroborative inquiry of management to determine that network audit settings were configured to log specific logon events on the domain.	No Exceptions Noted
	A third party application is used to monitor network devices and generate e-mail notifications when certain events occur. Logs are analyzed either manually or by automated tools to identify trends that may have a potential impact on LNRS' ability to achieve its system security objectives.	Inspected the monitoring applications and alerting configurations and conducted a corroborative inquiry of management to determine that the third-party application generated notifications when certain network device events occurred.	No Exceptions Noted

## Trust Services Principle – Common Criteria (Continued)

*Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC2.0 Common Criteria Related to Communication and Information (Continued)			
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	LNRS has documented job descriptions that describe the roles and responsibilities of the position.	Inspected the job descriptions for the sampled roles to determine they were in place and described the roles and responsibilities of the position.	No Exceptions Noted
	Security Planning and Maintenance responsibilities have been delegated.	Inspected the security planning delegation and conducted a corroborative inquiry of management to determine that responsibility for Security Planning and Maintenance had been delegated.	No Exceptions Noted
	A description of the system is posted on LNRS' intranet and is available to LNRS' internal users. This description delineates the boundaries of the system and key aspects of processing.	Inspected LNRS' intranet to determine a description of the system is posted on LNRS' intranet and is available to internal users.	No Exceptions Noted
	LNRS publishes its IT security policies on its corporate intranet.	Inspected LNRS' policies as posted on the internal SharePoint to determine LNRS publishes its IT security policies on its corporate intranet.	No Exceptions Noted
	LNRS has documented standard operating procedures to communicate the responsibilities and requirements in the operation of the system.	Inspected the example SOP documents and conducted corroborative inquiry of management to determine that standard operating procedures were documented and in place.	No Exceptions Noted



**Trust Services Principle – Common Criteria (Continued)***Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC2.0	Common Criteria Related to Communication and Information (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	Full-time employees are given Security Awareness training during their new hire orientation and are then updated on an annual basis.	Inspected the security awareness training logs for the sampled new hires and active employees to determine that staff were given Security Awareness training during their new hire orientation and then updated on an annual basis.	No Exceptions Noted
	Policies and procedures are in place to guide personnel on their responsibility for the handling of client information related to the secure storage and destruction of sensitive data and documents.	Inspected the Records Management Policy, the Information Value Classification Procedures, and conducted a corroborative inquiry of management to determine that policies were in place to guide personnel on their responsibility for the handling of client information related to the secure storage and destruction of sensitive data and documents.	No Exceptions Noted

## Trust Services Principle – Common Criteria (Continued)

*Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC2.0	Common Criteria Related to Communication and Information (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	A description of the system is posted on LNRS' Public Web Site and is available to users.	Inspected LNRS' public website to determine a description of the system is posted on LNRS' Public Web Site and is available to users.	No Exceptions Noted
	Maintenance contracts are in place with production hardware vendors that provide system support services and expedited parts delivery.	Inspected the maintenance agreements and invoices for the hardware vendors determine that maintenance contracts were in place with production server hardware vendors that provide system support services and expedited parts delivery.	No Exceptions Noted
	Methods for informing LNRS about breaches is posted to LNRS' intranet site.	Inspected the incident/breach reporting process as available on LNRS' intranet to determine that user requirements for informing LNRS about breaches was posted to LNRS' intranet site.	No Exceptions Noted
	Management has documented support operations procedures to outline how customer reported issues are addressed and resolved.	Inspected the support documentation and conducted a corroborative inquiry of management to determine that they were in place and current.	No Exceptions Noted

**Trust Services Principle – Common Criteria (Continued)***Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC2.0	Common Criteria Related to Communication and Information (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	Customer reported problems are entered into a trouble ticket system. Tickets are opened, investigated, and resolved per problem management procedures.	Inspected the support ticketing systems and conducted a corroborative inquiry of management to determine that the tickets were created, worked, and documented as described.	No Exceptions Noted
	The organization displays a sign-on banner before granting access to the system that provides privacy and security notices consistent with applicable system use policy.	Inspected the sign-on banner messages to determine the organization displays a sign-on banner before granting access to the system that provides privacy and security notices consistent with applicable system use policy.	No Exceptions Noted

**Trust Services Principle – Common Criteria (Continued)***Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC3.0	Common Criteria Related to Risk Assessment		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	LNRS has a risk management program to address security and business-related risks.	Inspected the Risk Assessment Process to determine that LNRS had a documented risk management program to address security and business-related risks.	No Exceptions Noted
	Risk Committee meetings are held periodically to monitor the controls of LNRS.	Inspected the Information Security Council meeting minutes to determine that the Risk Committee meetings were held periodically to monitor the controls of LNRS.	No Exceptions Noted

**Trust Services Principle – Common Criteria (Continued)***Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC3.0	Common Criteria Related to Risk Assessment (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	Risk Committee meetings are held periodically to monitor the controls of LNRS.	Inspected the Information Security Council meeting minutes to determine that the Risk Committee meetings were held periodically to monitor the controls of LNRS.	No Exceptions Noted
	LNRS completes a risk assessment and updates the list of identified risks periodically.	Inspected the risk assessment spreadsheets to determine that LNRS completed a risk assessment and updated the identified risks.	No Exceptions Noted
	LNRS assesses the risks that vendors and business partners will fail to meet LNRS's requirements.	Inspected the third-party risk considerations to determine that LNRS assessed the risks that vendors and business partners will fail to meet LNRS's requirements.	No Exceptions Noted
	LNRS has a Security Incident Response Policy and Procedures in place to provide policy guidance and establish responsibilities for responding to and reporting security breaches.	Inspected the Data Security Incident Response Overview and Incident Response and Notification Policy to determine that LNRS had a Security Incident Response Policy and Procedures in place to provide policy guidance for responding to and reporting security breaches.	No Exceptions Noted
	LNRS subscribes to security bulletins and notices for newly discovered vulnerabilities in order to identify patches to be applied.	Inspected the example security bulletins from third party specialists and conducted a corroborative inquiry of management to determine that LNRS subscribed to security bulletins and notices for newly discovered vulnerabilities in order to identify patches to be applied.	No Exceptions Noted

## Trust Services Principle – Common Criteria (Continued)

*Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC3.0	Common Criteria Related to Risk Assessment (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	Vulnerability assessments are performed by a third-party vendor periodically to test for known vulnerabilities on the network and production systems.	Inspected the third-party vulnerability assessment reports and conducted a corroborative inquiry of management to determine whether the assessments were performed as described.	No Exceptions Noted
	Vulnerability scans are performed on an ongoing basis by IT staff to test for known vulnerabilities on the network and production systems to facilitate scheduled reporting to stakeholders.	Inspected the vulnerability scanning logs for the sampled months and conducted a corroborative inquiry of management to determine the assessments were performed as described.	No Exceptions Noted

**Trust Services Principle – Common Criteria (Continued)***Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC3.0	Common Criteria Related to Risk Assessment (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	Risk Committee meetings are held periodically to monitor the controls of LNRS.	Inspected the Information Security Council meeting minutes to determine that the Risk Committee meetings were held periodically to monitor the controls of LNRS.	No Exceptions Noted
	LNRS completes a risk assessment and updates the list of identified risks periodically.	Inspected the risk assessment spreadsheets to determine that LNRS completed a risk assessment and updated the identified risks.	No Exceptions Noted
	LNRS considers fraud when completing its risk assessment.	Inspected the fraud considerations in the risk assessment to determine that LNRS included fraud within their risk assessment.	No Exceptions Noted



## Trust Services Principle – Common Criteria (Continued)

*Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC3.0	Common Criteria Related to Risk Assessment (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	LNRS completes a risk assessment and updates the list of identified risks periodically.	Inspected the risk assessment spreadsheets to determine that LNRS completed a risk assessment and updated the identified risks.	No Exceptions Noted
	LNRS assesses the risks that vendors and business partners will fail to meet LNRS's requirements.	Inspected the third-party risk considerations to determine that LNRS assessed the risks that vendors and business partners will fail to meet LNRS's requirements.	No Exceptions Noted
	Policies and procedures are in place for patch management on production systems.	Inspected the patch history for the sampled servers to determine that a patch management process was in place.	No Exceptions Noted
	LNRS' application program code is designed and documented in accordance with written standards and procedures established by management in the SDLC.	Inspected the Secure Software Development Lifecycle Standards and conducted a corroborative inquiry of management to determine that the phases of the systems development and maintenance processes were documented.	No Exceptions Noted
	Source code management software is utilized for version control of development projects and to control access to source code libraries.	Inspected the version control software tools and conducted a corroborative inquiry of management to determine that software was used to manage version control and access rights to the source code libraries.	No Exceptions Noted
	A tracking system is used to log critical and non-critical application change requests (issues/projects) reported by users or internal parties.	Inspected the change ticketing tracking system and conducted a corroborative inquiry of management to determine that a ticketing system was used.	No Exceptions Noted

## Trust Services Principle – Common Criteria (Continued)

*Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC3.0 Common Criteria Related to Risk Assessment (Continued)			
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	An Infrastructure Change Management Policy is in place to guide personnel on documenting and implementing change control procedures that affect production systems.	Inspected the Change Management Standard and conducted a corroborative inquiry of management to determine policies were in place to guide changes made to infrastructure.	No Exceptions Noted
	Changes to the production environment are documented in the ticketing system and a work order is created.	Inspected the tickets for a sample of infrastructure changes and firewall changes and conducted a corroborative inquiry of management to determine that changes were logged in a ticketing system.	No Exceptions Noted
	Management has documented support operations procedures to outline how customer reported issues are addressed and resolved.	Inspected the support documentation and conducted a corroborative inquiry of management to determine that they were in place and current.	No Exceptions Noted
	Customer reported problems are entered into a trouble ticket system. Tickets are opened, investigated, and resolved per problem management procedures.	Inspected the support ticketing systems and conducted a corroborative inquiry of management to determine that the tickets were created, worked, and documented as described.	No Exceptions Noted
	Escalation procedures are in place to assign tickets to technical or application personnel that required an elevated level of support.	Inspected the escalation process and conducted a corroborative inquiry of management to determine that tickets followed escalation procedures when required by the nature of the issue.	No Exceptions Noted

**Trust Services Principle – Common Criteria (Continued)***Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC4.0 Common Criteria Related to Monitoring Activities			
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	Management meetings are held on a regular basis to discuss operational issues.	Inspected the management meeting agendas and minutes throughout the audit period to determine that management meetings were held on a regular basis to discuss operational issues.	No Exceptions Noted
	Internal auditing of LNRS' processes is performed periodically.	Inspected the internal auditing schedules to determine that periodic internal auditing was performed.	No Exceptions Noted
	Employee evaluations are performed on a regular basis against individual objectives derived from LNRS' goals, established standards, and specific job responsibilities.	Inspected the evaluations for the sample selected active employees to determine that employee evaluations were performed on a regular basis against individual objectives derived from the organization's goals, established standards, and specific job responsibilities.	No Exceptions Noted
	Systems Logs and Audit Trails are restricted and protected from unauthorized access and deletion.	Inspected the restrictions on the ability to modify or purge logs and conducted a corroborative inquiry of management to determine that system logs and audit trails were protected from unauthorized access and deletion.	No Exceptions Noted

**Trust Services Principle – Common Criteria (Continued)***Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC4.0 Common Criteria Related to Monitoring Activities (Continued)			
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate, as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	A third party application is used to monitor network devices and generate e-mail notifications when certain events occur. Logs are analyzed either manually or by automated tools to identify trends that may have a potential impact on LNRS' ability to achieve its system security objectives.	Inspected the monitoring applications and alerting configurations and conducted a corroborative inquiry of management to determine that the third-party application generated notifications when certain network device events occurred.	No Exceptions Noted
	Vulnerability assessments are performed by a third-party vendor periodically to test for known vulnerabilities on the network and production systems.	Inspected the third-party vulnerability assessment reports and conducted a corroborative inquiry of management to determine whether the assessments were performed as described.	No Exceptions Noted
	Vulnerability scans are performed on an ongoing basis by IT staff to test for known vulnerabilities on the network and production systems to facilitate scheduled reporting to stakeholders.	Inspected the vulnerability scanning logs for the sampled months and conducted a corroborative inquiry of management to determine the assessments were performed as described.	No Exceptions Noted
	Vulnerability assessments are performed by a third-party vendor periodically to assess vulnerabilities to the network and production systems.	Inspected the vulnerability scanning and penetration testing reports to determine vulnerability assessments are performed by a third-party vendor periodically to assess vulnerabilities to the network and production systems.	No Exceptions Noted

**Trust Services Principle – Common Criteria (Continued)***Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC4.0 Common Criteria Related to Monitoring Activities (Continued)			
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate, as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	Network Penetration tests are performed by IT staff periodically to gain unauthorized access to the network and production systems.	Inspected the penetration testing reports to determine network penetration tests are performed by IT staff periodically to gain unauthorized access to the network and production systems.	No Exceptions Noted
	LNRS has a Security Incident Response Policy and Procedures in place to provide policy guidance and establish responsibilities for responding to and reporting security breaches.	Inspected the Data Security Incident Response Overview and Incident Response and Notification Policy to determine that LNRS had a Security Incident Response Policy and Procedures in place to provide policy guidance for responding to and reporting security breaches.	No Exceptions Noted
	The Development team has adopted OWASP-based standards for building, designing, and testing the security of web applications and web services.	Inspected the SDLC Policy and the Baselines Application Security Requirements and conducted a corroborative inquiry of management to determine to determine that OWASP Top 10 testing was performed for development and maintenance activities.	No Exceptions Noted

## Trust Services Principle – Common Criteria (Continued)

*Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC5.0	Common Criteria Related to Control Activities		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	LNRS completes a risk assessment and updates the list of identified risks periodically.	Inspected the risk assessment spreadsheets to determine that LNRS completed a risk assessment and updated the identified risks.	No Exceptions Noted
	LNRS is segregated into separate and distinct functional areas for the purposes of the management and processing of customer information.	Inspected the organizational chart to determine that the organization was segregated into separate, logical, and distinct functional areas for the purpose of management and processing of customer information.	No Exceptions Noted
	A firewall is in place to control network traffic and prevent unauthorized traffic from passing between the internal network and external networks.	Inspected the configured firewalls and conducted a corroborative inquiry of management to determine that a firewall was in place to control network traffic and prevent unauthorized traffic from passing between the internal network and external networks.	No Exceptions Noted
	A redundant firewall is in place and has been configured as a standby to the primary firewall.	Inspected the redundant firewall configurations and conducted a corroborative inquiry of management to determine that a redundant firewall was in place and has been configured as a fail over.	No Exceptions Noted
	Management restricts the ability to administer the firewall systems and network communications equipment to certain personnel.	Inspected the firewall administrators and conducted a corroborative inquiry of management to determine that management restricts the ability to administer the firewall systems and network communications equipment to certain personnel.	No Exceptions Noted

## Trust Services Principle – Common Criteria (Continued)

*Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC5.0	Common Criteria Related to Control Activities		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	Direct access to the firewall is restricted to a predefined set of IP addresses, and communications are encrypted.	Inspected the direct access IP address restrictions and encryption configurations and conducted a corroborative inquiry of management to determine that direct access to the firewall was restricted to a predefined set of IP addresses and that communications were encrypted.	No Exceptions Noted
	The firewall is configured to automatically terminate authenticated sessions to the firewall if predefined inactivity thresholds are exceeded.	Inspected the firewall idle time out configurations and conducted a corroborative inquiry of management to determine that it was configured to automatically terminate authenticated sessions to the firewall if predefined inactivity thresholds were exceeded.	No Exceptions Noted
	The firewall is configured to generate e-mail notifications when certain firewall events occur.	Inspected the firewall email alerts and conducted a corroborative inquiry of management to determine that it was configured to send notifications to administrators when certain events occurred.	No Exceptions Noted
	An Intrusion Prevention Systems (IPS) is utilized to continuously monitor the network for malicious activity and unauthorized access attempts.	Inspected the IPS configuration, the log history, and conducted a corroborative inquiry of management to determine that a IPS was in place, monitoring the network continuously, and provided alert to administrators.	No Exceptions Noted



## Trust Services Principle – Common Criteria (Continued)

*Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC5.0	Common Criteria Related to Control Activities		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	A DMZ is in place for web facing systems and is logically separate from the internal production network.	Inspected the DMZs and conducted a corroborative inquiry of management to determine that a DMZ was in use for certain server systems.	No Exceptions Noted
	LNRS conducts facility maintenance and reviews the adequacy of the physical access controls.	Inspected the Physical Security policies, equipment maintenance and monitoring agreements, and the physical security walkthrough logs to determine LNRS conducts facility maintenance and reviews the adequacy of the physical access controls.	No Exceptions Noted

## Trust Services Principle – Common Criteria (Continued)

*Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC5.0	Common Criteria Related to Control Activities (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	Security Planning and Maintenance responsibilities have been delegated.	Inspected the security planning delegation and conducted a corroborative inquiry of management to determine that responsibility for Security Planning and Maintenance had been delegated.	No Exceptions Noted
	Monitoring audits of all user account rights assignments are performed periodically to ensure staff have the correct level of access to target systems for their job responsibilities.	Inspected the user access review schedules, auditing tool, email notification, and conducted a corroborative inquiry of management to determine the audits were performed to monitor user access rights assignments.	No Exceptions Noted
	Privileged Account Access procedures are in place to ensure privileged accounts are used for system administrative purposes only and to prevent user level tasks from being performed using privileged accounts.	Inspected the User Access Control Procedures and the separate administrative and non-administrative accounts and conducted a corroborative inquiry of management to determine that Privileged Account Access procedures were in place to ensure privileged accounts were used for system administrative purposes only and to prevent user level tasks from being performed using privileged accounts.	No Exceptions Noted
	Administration rights to databases are restricted to only authorized personnel.	Inspected the authorized users for database access and conducted a corroborative inquiry of management to determine that access was restricted to only certain authorized administrators.	No Exceptions Noted

**Trust Services Principle – Common Criteria (Continued)***Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC5.0	Common Criteria Related to Control Activities (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	Administration and user level rights to production applications are restricted and monitored.	Inspected the application-level user access review logs and conducted a corroborative inquiry of management to determine that user account management practices were in place to restrict and monitor access to the applications.	No Exceptions Noted
	Policies and procedures are in place for patch management on production systems.	Inspected the patch history for the sampled servers to determine that a patch management process was in place.	No Exceptions Noted
	LNRS has developed strategic IT Plans which are aligned with Business Objectives.	Inspected the strategic IT planning and review documentation to determine LNRS has developed strategic IT Plans which are aligned with Business Objectives.	No Exceptions Noted
	LNRS has established load balancing on certain systems to ensure high availability and a responsive end user experience.	Inspected the configured load balancing server pools to determine that load balancing had been implemented to ensure high availability and a pleasant end-user experience.	No Exceptions Noted
	A monitoring application is utilized to monitor network devices and critical systems.	Inspected the monitoring tools dashboards and available reports to determine that the organization utilized monitoring applications to measure production systems utilization and availability.	No Exceptions Noted

## Trust Services Principle – Common Criteria (Continued)

*Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC5.0	Common Criteria Related to Control Activities (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	Monitoring applications send e-mail alert notifications to operations personnel when predefined thresholds are exceeded on monitored network devices.	Inspected the samples of email alert notifications to determine that sufficient notification takes place when predefined thresholds are exceeded.	No Exceptions Noted
	The network communications infrastructure is configured with redundant components and diverse path switching.	Inspected the redundant network equipment configurations to determine that certain components have redundancy to ensure high availability.	No Exceptions Noted
	File-integrity monitoring (FIM) software is configured to detect and log modifications to critical system and application files.	Inspected the integrity log monitoring for the sampled servers to determine that File-integrity monitoring software was configured to alert operations personnel to unauthorized modifications to critical system files and databases.	No Exceptions Noted
	Antivirus software is present on production servers and workstations and conducts regular system scans.	Inspected the antivirus configuration for the sampled workstations and servers to determine that countermeasures have been established and implemented to detect and remove malicious code.	No Exceptions Noted
	Antivirus software is configured to automatically update servers and personal computers on a daily basis.	Inspected the centralized antivirus update configurations to determine antivirus software was configured to automatically update servers and workstations.	No Exceptions Noted

## Trust Services Principle – Common Criteria (Continued)

*Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC5.0	Common Criteria Related to Control Activities (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	The clocks of all relevant information processing systems within LNRS are synchronized with an accurate time source.	Inspected the time sync configuration for the selected servers and conducted a corroborative inquiry of management to determine that the system clocks of all relevant information processing systems within LNRS were synchronized with an accurate time source.	No Exceptions Noted
	An application is used to identify authorized and unauthorized devices connecting to the network.	Inspected the rogue access scans and the new device reporting functionality to determine that LNRS had automated applications to identify authorized and unauthorized devices connecting to the network.	No Exceptions Noted
	Management has developed the IT Strategic Plan to align with Business Objectives.	Inspected the plan documents and conducted inquiry of management to determine that management had developed the IT Strategic Plan to align with Business Objectives.	No Exceptions Noted
	LNRS has an Information Assurance and Data Protection Review Board which oversees IT planning and IT functions.	Inspected the Technology, Risk, and Data Services month end close meeting minutes/report to determine LNRS has an Information Assurance and Data Protection Review Board which oversees IT planning and IT functions.	No Exceptions Noted
	Information Assurance and Data Protection Review Board meet regularly and communicate findings to senior management.	Inspected the Technology, Risk, and Data Services month end close meeting minutes/report to determine the Information Assurance and Data Protection Review Board meet regularly and communicate findings to senior management.	No Exceptions Noted

## Trust Services Principle – Common Criteria (Continued)

*Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC5.0 Common Criteria Related to Control Activities (Continued)			
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	The Information Assurance and Data Protection Review Board monitors the IT Strategic Plan through performance reporting and budgeting.	Inspected the Technology, Risk, and Data Services month end close meeting minutes/report to determine the Information Assurance and Data Protection Review Board monitors the IT Strategic Plan through performance reporting and budgeting.	No Exceptions Noted
	Continuous Improvement Programs as in place to evaluate, monitor and adjust LNRS' Information Security Program.	Inspected the continuous improvement program supporting documentation to determine a program was in place to evaluate, monitor, and adjust LNRS' Information Security Program.	No Exceptions Noted
	LNRS has established an Information Security Management Program to manage, monitor, maintain and improve Information Security in LNRS	Inspected the Information Security Policy, the Information Security Council Charter, the Information Assurance and Data Protection Governance Model and Charter, and the internal audit and risk management documentation to determine that LNRS had an Information Security Management Program.	No Exceptions Noted

## Trust Services Principle – Common Criteria (Continued)

*Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC5.0	Common Criteria Related to Control Activities (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	LNRS. has an Information Security Policy that describes the security posture and practices of LNRS.	Inspected the Information Security Policy to determine that it was in place and described the security posture and practices of LNRS.	No Exceptions Noted
	The Information Security Policy is reviewed annually, updated, and approved by management to remain current.	Inspected the Information Security Policy review date to determine that LNRS policies were reviewed, updated, and approved by management within the previous twelve months.	No Exceptions Noted
	Employees acknowledge acceptance of IT Security Policies as part of the onboarding process.	Inspected the acknowledgements of security policies as included the offer letter for the sampled new hire employees to determine that employees must sign a statement confirming acknowledgment of all policies and procedures in the IT Security Policies.	No Exceptions Noted
	LNRS has policies and procedures governing physical security controls that limit access to the facility to authorized individuals.	Inspected the Physical Security Program to determine that LNRS had policies and procedures governing physical security controls that limit access to the facility to authorized individuals.	No Exceptions Noted
	Management maintains documented backup schedules, policies, and procedures.	Inspected the Data Backup Policy to determine that it was in place as described.	No Exceptions Noted



**Trust Services Principle – Common Criteria (Continued)***Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC5.0	Common Criteria Related to Control Activities (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	LNRS has a Security Incident Response Policy and Procedures in place to provide policy guidance and establish responsibilities for responding to and reporting security breaches.	Inspected the Data Security Incident Response Overview and Incident Response and Notification Policy to determine that LNRS had a Security Incident Response Policy and Procedures in place to provide policy guidance for responding to and reporting security breaches.	No Exceptions Noted
	Management maintains documented account management policies and procedures to provide guidance on the management of user accounts on target systems and password standards.	Inspected the User Access Control Procedures to determine the policies and procedures for account management and password configuration are in place and provide guidance on logical access requirements.	No Exceptions Noted
	Network Access and Authentication Policies are used to ensure that users connecting to the corporate network are authenticated in an appropriate manner.	Inspected Authentication and Authorization section of the Computer Network Security Policy to determine Network Access and Authentication Policies are used to ensure that users connecting to the corporate network are authenticated in an appropriate manner.	No Exceptions Noted
	Management maintains a data encryption policy and procedure that provides guidance on LNRS' standards for data at rest, sending, and receiving sensitive information.	Inspected the Encryption Policy and Standard and conducted a corroborative inquiry of management to determine the policies and guidance for data encryption have been established.	No Exceptions Noted

## Trust Services Principle – Common Criteria (Continued)

*Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC5.0	Common Criteria Related to Control Activities (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	Management maintains a disaster recovery plan (DRP) to facilitate disaster recovery operations.	Inspected the Technical Resilience Program, the Business Continuity Management Policy, and conducted a corroborative inquiry of management to determine that it was in place to facilitate disaster recovery operations.	No Exceptions Noted
	Policies and procedures are in place to guide personnel on their responsibility for the privacy and confidentiality of data and documents, and the allowed methods and purposes for disclosure.	Inspected the Electronic Content Policy and the Information Value Classification Policy and Procedures to determine that policies were in place to guide personnel on their responsibility for the privacy/confidentiality of documents and data and the allowed methods and purposes of such disclosure if any.	No Exceptions Noted
	Policies and procedures are in place to guide personnel on their responsibility for the handling of client information related to the secure storage and destruction of sensitive data and documents.	Inspected the Records Management Policy, the Information Value Classification Procedures, and conducted a corroborative inquiry of management to determine that policies were in place to guide personnel on their responsibility for the handling of client information related to the secure storage and destruction of sensitive data and documents.	No Exceptions Noted
	LNRS' application program code is designed and documented in accordance with written standards and procedures established by management in the SDLC.	Inspected the Secure Software Development Lifecycle Standards and conducted a corroborative inquiry of management to determine that the phases of the systems development and maintenance processes were documented.	No Exceptions Noted

## Trust Services Principle – Common Criteria (Continued)

*Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC5.0	Common Criteria Related to Control Activities (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	An Infrastructure Change Management Policy is in place to guide personnel on documenting and implementing change control procedures that affect production systems.	Inspected the Change Management Standard and conducted a corroborative inquiry of management to determine policies were in place to guide changes made to infrastructure.	No Exceptions Noted
	Management has documented support operations procedures to outline how customer reported issues are addressed and resolved.	Inspected the support documentation and conducted a corroborative inquiry of management to determine that they were in place and current.	No Exceptions Noted

## Trust Services Principle – Common Criteria (Continued)

*Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC6.0 Common Criteria Related to Logical and Physical Access Controls			
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	IT access request tickets are used to ensure new staff receive the appropriate level of access to information systems and facilities.	Inspected the access request tickets for the sampled new hire employees to determine that new hire checklists were used to ensure that new staff receives the appropriate level of access to information systems and facilities.	No Exceptions Noted
	Access to modify backup jobs and backup job notification settings is restricted to authorized personnel.	Inspected the authorized backup administrators and conducted a corroborative inquiry of management to determine that access to make changes to the backup jobs and backup notification settings was restricted to authorized personnel.	No Exceptions Noted
	LNRS maintains technology asset lists to identify assets that require protection against threats.	Inspected the IT asset management tools to determine that LNRS maintained technology asset lists to identify assets that required protection against threats.	No Exceptions Noted
	Management maintains documented account management policies and procedures to provide guidance on the management of user accounts on target systems and password standards.	Inspected the User Access Control Procedures to determine the policies and procedures for account management and password configuration are in place and provide guidance on logical access requirements.	No Exceptions Noted
	Network users are authenticated via an authorized network ID and password before being granted access to the network domain.	Inspected the network authentication mechanism to determine that network users were authenticated via an authorized network ID and password before being granted access to the network.	No Exceptions Noted

## Trust Services Principle – Common Criteria (Continued)

*Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC6.0 Common Criteria Related to Logical and Physical Access Controls			
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	Passwords must conform to minimum requirements as enforced by the network operating system. Password complexity standards are established to enforce control over access control software passwords.	Inspected the configured password requirements and conducted a corroborative inquiry of management to determine that network passwords conform to the requirements.	No Exceptions Noted
	Network domain administrator rights are restricted to specific network operations personnel.	Inspected the domain administrators and conducted a corroborative inquiry of management to determine that network administrator rights were restricted to certain authorized personnel as described.	No Exceptions Noted
	Security groups have been configured and are enforced by the network operating system and servers to ensure access is restricted to sensitive data stored on the network.	Inspected the configured security groups and conducted a corroborative inquiry of management to determine that security groups were in use that restricted access to sensitive data stored on the network.	No Exceptions Noted
	Monitoring audits of all user account rights assignments are performed periodically to ensure staff have the correct level of access to target systems for their job responsibilities.	Inspected the user access review schedules, auditing tool, email notification, and conducted a corroborative inquiry of management to determine the audits were performed to monitor user access rights assignments.	No Exceptions Noted

## Trust Services Principle – Common Criteria (Continued)

*Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC6.0 Common Criteria Related to Logical and Physical Access Controls			
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	Administration rights to databases are restricted to only authorized personnel.	Inspected the authorized users for database access and conducted a corroborative inquiry of management to determine that access was restricted to only certain authorized administrators.	No Exceptions Noted
	Administration and user level rights to production applications are restricted and monitored.	Inspected the application-level user access review logs and conducted a corroborative inquiry of management to determine that user account management practices were in place to restrict and monitor access to the applications.	No Exceptions Noted
	Privileged Account Access procedures are in place to ensure privileged accounts are used for system administrative purposes only and to prevent user level tasks from being performed using privileged accounts.	Inspected the User Access Control Procedures and the separate administrative and non-administrative accounts and conducted a corroborative inquiry of management to determine that Privileged Account Access procedures were in place to ensure privileged accounts were used for system administrative purposes only and to prevent user level tasks from being performed using privileged accounts.	No Exceptions Noted
	Systems Logs and Audit Trails are restricted and protected from unauthorized access and deletion.	Inspected the restrictions on the ability to modify or purge logs and conducted a corroborative inquiry of management to determine that system logs and audit trails were protected from unauthorized access and deletion.	No Exceptions Noted

## Trust Services Principle – Common Criteria (Continued)

*Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC6.0 Common Criteria Related to Logical and Physical Access Controls			
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	Databases containing sensitive data are encrypted.	Inspected the database encryption configurations and conducted an inquiry of management to determine that databases containing sensitive data were encrypted.	No Exceptions Noted
	Access to Privileged Utility Programs is restricted to authorized users.	Inspected the logical access controls to determine access to Privileged Utility Programs is restricted to authorized users.	No Exceptions Noted
	Documented standards are in place and followed for the proper maintenance and operation of firewalls used on perimeter networks.	Inspected the Secure Firewall Procedures and Infrastructure Security Architecture and conducted a corroborative inquiry of management to determine that documented standards were in place and followed for the proper maintenance and operation of firewalls used on perimeter networks.	No Exceptions Noted
	Firewall rules are monitored on an ongoing basis and changes to configurations trigger alerts to personnel to ensure appropriate and accurate configuration settings are maintained.	Inspected the firewall review meeting event, the example email alerts, and conducted a corroborative inquiry of management to determine that Router and Firewall rules were reviewed every 6 months to ensure settings have not been modified.	No Exceptions Noted
	Network Segmentation is used to protect sensitive information and to manage servers and workstations in similar groupings.	Inspected the configured vlans and conducted a corroborative inquiry of management to determine that network segmentation was used to protect sensitive information.	No Exceptions Noted

## Trust Services Principle – Common Criteria (Continued)

*Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC6.0 Common Criteria Related to Logical and Physical Access Controls			
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	Management maintains a data encryption policy and procedure that provides guidance on LNRS' standards for data at rest, sending, and receiving sensitive information.	Inspected the Encryption Policy and Standard and conducted a corroborative inquiry of management to determine the policies and guidance for data encryption have been established.	No Exceptions Noted
	Management maintains a remote access policy and procedure that provides guidance on LNRS' standards for administering connections to and from remote networks.	Inspected the Remote Access Policy to determine the policies and procedures are in place to guide securely access to and from remote networks.	No Exceptions Noted
	Remote connections to the corporate network are configured to automatically terminate after idle time-outs have been reached.	Inspected the remote user VPN idle timeout configuration to determine remote connections to the corporate network are configured to automatically terminate after idle time-outs have been reached.	No Exceptions Noted



**Trust Services Principle – Common Criteria (Continued)***Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC6.0 Common Criteria Related to Logical and Physical Access Controls			
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	A clear desk policy for papers, removable storage media and a clear screen policy for information processing facilities is in place. Users are aware of their responsibility for ensuring unattended equipment is secure from unauthorized access.	Inspected the Secure Workspace Policy, the centralized workstation idle timeout configuration, and conducted a corroborative inquiry of management to determine that a clear desk policy for papers, removable storage media and a clear screen policy for information processing facilities was in place.	No Exceptions Noted
	Management requires disk level encryption for laptops, portable devices and media.	Inspected the disk level encryption for the sampled laptops and conducted a corroborative inquiry of management to determine that management required disk level encryption for laptops, portable devices and media.	No Exceptions Noted

## Trust Services Principle – Common Criteria (Continued)

*Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC6.0	Common Criteria Related to Logical and Physical Access Controls (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users, whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.		
	IT access request tickets are used to ensure new staff receive the appropriate level of access to information systems and facilities.	Inspected the access request tickets for the sampled new hire employees to determine that new hire checklists were used to ensure that new staff receives the appropriate level of access to information systems and facilities.	No Exceptions Noted
	Management utilizes and retains termination tickets as confirmation of the revocation of system and facility access privileges as a component of the employee termination process.	Inspected the completed termination checklists for the sample selected terminated employees to determine that management utilized termination checklists as confirmation of revocation of the system and facility access privileges when terminated.	No Exceptions Noted
	Security group audits are performed three times annually on production servers to ensure that the appropriate security groups and group memberships are defined, any variances are identified and corrected.	Inspected the security group audit emails and tracking logs and conducted a corroborative inquiry of management to determine the audits were performed to ensure that the appropriate security groups and group memberships were defined.	No Exceptions Noted

**Trust Services Principle – Common Criteria (Continued)***Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC6.0 Common Criteria Related to Logical and Physical Access Controls (Continued)			
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users, whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.		
	Monitoring audits of all user account rights assignments are performed periodically to ensure staff have the correct level of access to target systems for their job responsibilities.	Inspected the user access review schedules, auditing tool, email notification, and conducted a corroborative inquiry of management to determine the audits were performed to monitor user access rights assignments.	No Exceptions Noted
	Termination procedures are in place for the removal of access to all systems upon notification of the termination.	Inspected termination procedure and access removal process for the sampled terminated employees and conducted a corroborative inquiry of management to determine that terminated employee's access was revoked.	No Exceptions Noted

## Trust Services Principle – Common Criteria (Continued)

*Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC6.0 Common Criteria Related to Logical and Physical Access Controls (Continued)			
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, considering the concepts of least privilege and segregation of duties, to meet the entity's objectives.		
	Management utilizes and retains termination tickets as confirmation of the revocation of system and facility access privileges as a component of the employee termination process.	Inspected the completed termination checklists for the sample selected terminated employees to determine that management utilized termination checklists as confirmation of revocation of the system and facility access privileges when terminated.	No Exceptions Noted
	Termination procedures are in place for the removal of access to all systems upon notification of the termination.	Inspected termination procedure and access removal process for the sampled terminated employees and conducted a corroborative inquiry of management to determine that terminated employee's access was revoked.	No Exceptions Noted
	IT access request tickets are used to ensure new staff receive the appropriate level of access to information systems and facilities.	Inspected the access request tickets for the sampled new hire employees to determine that new hire checklists were used to ensure that new staff receives the appropriate level of access to information systems and facilities.	No Exceptions Noted
	Monitoring audits of all user account rights assignments are performed periodically to ensure staff have the correct level of access to target systems for their job responsibilities.	Inspected the user access review schedules, auditing tool, email notification, and conducted a corroborative inquiry of management to determine the audits were performed to monitor user access rights assignments.	No Exceptions Noted
	Security groups have been configured and are enforced by the network operating system and servers to ensure access is restricted to sensitive data stored on the network.	Inspected the configured security groups and conducted a corroborative inquiry of management to determine that security groups were in use that restricted access to sensitive data stored on the network.	No Exceptions Noted

## Trust Services Principle – Common Criteria (Continued)

*Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC6.0	Common Criteria Related to Logical and Physical Access Controls (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, considering the concepts of least privilege and segregation of duties, to meet the entity's objectives.		
	Privileged Account Access procedures are in place to ensure privileged accounts are used for system administrative purposes only and to prevent user level tasks from being performed using privileged accounts.	Inspected the User Access Control Procedures and the separate administrative and non-administrative accounts and conducted a corroborative inquiry of management to determine that Privileged Account Access procedures were in place to ensure privileged accounts were used for system administrative purposes only and to prevent user level tasks from being performed using privileged accounts.	No Exceptions Noted
	User change procedures are in place for the change of access to all systems upon notification of a user role change.	Inspected the Change Management Standard and the User Access Control Procedures and conducted a corroborative inquiry of management to determine that user profile change procedures were in place.	No Exceptions Noted
	Policies and procedures are in place to guide personnel on their responsibility for the handling of client information related to the secure storage and destruction of sensitive data and documents.	Inspected the Records Management Policy, the Information Value Classification Procedures, and conducted a corroborative inquiry of management to determine that policies were in place to guide personnel on their responsibility for the handling of client information related to the secure storage and destruction of sensitive data and documents.	No Exceptions Noted

## Trust Services Principle – Common Criteria (Continued)

*Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC6.0 Common Criteria Related to Logical and Physical Access Controls (Continued)			
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	Management utilizes and retains termination tickets as confirmation of the revocation of system and facility access privileges as a component of the employee termination process.	Inspected the completed termination checklists for the sample selected terminated employees to determine that management utilized termination checklists as confirmation of revocation of the system and facility access privileges when terminated.	No Exceptions Noted
	LNRS has policies and procedures governing physical security controls that limit access to the facility to authorized individuals.	Inspected the Physical Security Program to determine that LNRS had policies and procedures governing physical security controls that limit access to the facility to authorized individuals.	No Exceptions Noted
	Entrances to the facility remain locked or monitored at all times and access is restricted to authorized personnel.	Observed the entrance controls during onsite procedures to determine that entrances to the facility remained locked or monitored at all times and access was restricted to authorized personnel.	No Exceptions Noted
	Visitors are required to check in with security and may not enter the building unless accompanied by an employee.	Observed the supervised entry during onsite procedures to determine that visitors were required to check in with security and were accompanied by an employee during their visit.	No Exceptions Noted
	Visitors are required to sign a visitor log and are issued a visitor badge which must be displayed by the visitor while on the premises.	Observed the visitor log during onsite procedures to determine that visitors were required to sign a visitor log, were issued a visitor badge.	No Exceptions Noted

**Trust Services Principle – Common Criteria (Continued)***Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC6.0	Common Criteria Related to Logical and Physical Access Controls (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	Visitors are required to wear badges and must be accompanied at all times.	Observed the visitor entry process during onsite procedures and conducted a corroborative inquiry of management to determine that visitors were required to wear badges and were accompanied at all times.	No Exceptions Noted
	Security guards are onsite to provide local security presence, screen and check-in all visitors, and monitor facility security systems.	Observed the security guard during onsite procedures to determine that security guards were onsite to provide local security presence, screened and check-in all visitors, and monitored facility security systems.	No Exceptions Noted
	Spare badges are kept in a secure location.	Observed the spare badge storage during onsite procedures to determine that spare keys to the facility were locked in a secure area.	No Exceptions Noted
	Management utilizes a badge access system to limit access to and within LNRS' facilities.	Observed the badge system during onsite procedures to determine that it was in place and restricted access to the facilities.	No Exceptions Noted
	Management restricts the ability to create, modify, or delete user badge access privileges to the facility.	Inspected the badge system administrators to determine that access to make changes to the facility access control system is restricted to authorized individuals. Inspected list of authorized individuals who can make changes to the facility access control system.	No Exceptions Noted

## Trust Services Principle – Common Criteria (Continued)

*Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC6.0 Common Criteria Related to Logical and Physical Access Controls (Continued)			
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	The access control system has the ability to generate entry and exit reports for review as necessary.	Inspected example entry reports to determine that the access control system can generate entry and exit reports for ad hoc review.	No Exceptions Noted
	All entrances to the data center remain locked at all times. Access is restricted and requires two-factor authentication.	Observed the entrance controls during onsite procedures to determine that entry controls were instituted and enforced.	No Exceptions Noted
	The walls surrounding the data center extend above the drop ceiling tiles all the way to the physical ceiling in order to prevent unauthorized access to restricted areas.	Observed the data center layout during onsite procedures to determine that the walls surrounding the data center extended above the drop ceiling tiles up to the physical ceiling.	No Exceptions Noted
	Man traps are used in the data center as an additional security measure prior to gaining access to the data center floor. The interior door remains locked until the exterior door is closed.	Observed the man traps during onsite procedures to determine that man traps were used in the data center as an additional security measure prior to gaining access to the data center floor. The interior door remained locked until the exterior door was closed.	No Exceptions Noted
	Employees are required to wear ID badges at all times in the facility.	Observed the badges in use during onsite procedures to determine that employees were required to wear ID badges at all times in the facility.	No Exceptions Noted



## Trust Services Principle – Common Criteria (Continued)

*Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC6.0 Common Criteria Related to Logical and Physical Access Controls (Continued)			
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	The badge access system has been configured with restricted zones for critical areas that require an elevated level of access.	Inspected the configured zones and access profiles to determine that the badge access system had been configured with restricted zones for critical areas that required an elevated level of access.	No Exceptions Noted
	Surveillance cameras record activities at the facility entrances and other areas within the facility.	Observed the surveillance cameras during onsite procedures to determine that surveillance cameras recorded activities at the facility entrances and other areas within the facility.	No Exceptions Noted
	Surveillance camera recordings are maintained for a certain number of days, allowing the capability for ad hoc review and investigations.	Observed the historic recordings during onsite procedures to determine surveillance camera recordings were maintained for a certain number of days, allowing the capability for ad hoc review and investigations.	No Exceptions Noted
	Security walkthroughs are performed periodically to monitor and check physical security as well as monitor health status of environmental systems.	Inspected the security walkthrough logs for the sampled dates to determine security walkthroughs are performed periodically to monitor and check physical security as well as monitor health status of environmental systems.	No Exceptions Noted
	Access to Delivery and Loading Areas is restricted, isolated and monitored.	Observed the delivery and loading area controls during onsite procedures to determine access to Delivery and Loading Areas is restricted, isolated and monitored.	No Exceptions Noted

## Trust Services Principle – Common Criteria (Continued)

*Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC6.0	Common Criteria Related to Logical and Physical Access Controls (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	Policies and procedures are in place to guide personnel on their responsibility for the classification of data and documents.	Inspected the Information Value Classification Policy and Procedures and conducted a corroborative inquiry of management to determine that policies were in place to guide personnel on their responsibility for the classification of documents and data related to the secure storage and destruction of sensitive data and documents.	No Exceptions Noted
	Policies and procedures are in place to guide personnel on their responsibility for the retention of data and documents.	Inspected the Record Retention Schedule and conducted a corroborative inquiry of management to determine that policies were in place to guide personnel on their responsibility for the retention of documents and data related to the secure storage and destruction of sensitive data and documents.	No Exceptions Noted
	Policies and procedures are in place to guide personnel on their responsibility for the privacy and confidentiality of data and documents, and the allowed methods and purposes for disclosure.	Inspected the Electronic Content Policy and the Information Value Classification Policy and Procedures to determine that policies were in place to guide personnel on their responsibility for the privacy/confidentiality of documents and data and the allowed methods and purposes of such disclosure if any.	No Exceptions Noted
	Secured areas and shredding bins are utilized for the storage of sensitive documents and those awaiting destruction by a contracted third party shredding vendor.	Observed the secured shredding bins during onsite procedures and conducted a corroborative inquiry of management to determine that documents awaiting destruction were kept in secured locations.	No Exceptions Noted

## Trust Services Principle – Common Criteria (Continued)

*Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC6.0	Common Criteria Related to Logical and Physical Access Controls (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	A third party vendor periodically retrieves and shreds sensitive documents contained in the secured containers.	Inspected the third party shredding invoices and conducted a corroborative inquiry of management to determine that the service was used.	No Exceptions Noted
	Documented procedures are in place to ensure all media are physically destroyed rendering all sensitive information unreadable before being discarded or recycled.	Inspected the Data Destruction Standards and an example certificate of destruction for physical media to determine that all a policy exists to guide personnel to destroy sensitive information before discarding assets.	No Exceptions Noted

## Trust Services Principle – Common Criteria (Continued)

*Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC6.0 Common Criteria Related to Logical and Physical Access Controls (Continued)			
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	Management maintains documented account management policies and procedures to provide guidance on the management of user accounts on target systems and password standards.	Inspected the User Access Control Procedures to determine the policies and procedures for account management and password configuration are in place and provide guidance on logical access requirements.	No Exceptions Noted
	Remote access to the network requires dual factor authentication.	Inspected the remote access authentication process and conducted inquiry of management to determine that remote access to the network requires dual factor authentication.	No Exceptions Noted
	A firewall is in place to control network traffic and prevent unauthorized traffic from passing between the internal network and external networks.	Inspected the configured firewalls and conducted a corroborative inquiry of management to determine that a firewall was in place to control network traffic and prevent unauthorized traffic from passing between the internal network and external networks.	No Exceptions Noted
	SFTP / FTPs servers are utilized for encrypted file transfers and is monitored and administered by the IT department.	Inspected the SFTP server configurations and conducted a corroborative inquiry of management to determine that the server was being utilized as described.	No Exceptions Noted
	Secure communication tunnels are in place for interactive web sites and file transfers requiring encryption to LNRS' servers through the use of SSL/TLS encryption.	Inspected the web server encryption certificates and conducted a corroborative inquiry of management to determine that the server was being utilized as described.	No Exceptions Noted

## Trust Services Principle – Common Criteria (Continued)

*Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC6.0 Common Criteria Related to Logical and Physical Access Controls (Continued)			
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	Contractor accounts used for remote access are formally approved and monitored by Information Technology personnel.	Inspected the remote access tracking tickets and approvals for a sample of contractor accounts and conducted a corroborative inquiry of management to determine that contractor accounts used for remote access are formally approved and monitored by Information Technology personnel.	No Exceptions Noted
	A DMZ is in place for web facing systems and is logically separate from the internal production network.	Inspected the DMZs and conducted a corroborative inquiry of management to determine that a DMZ was in use for certain server systems.	No Exceptions Noted
	Encrypted VPNs are utilized for remote access for the security and integrity of the data passing over the public network.	Inspected the site to site and remote user VPN settings and conducted a corroborative inquiry of management to determine that VPNs are in use.	No Exceptions Noted
	Site to site VPN connections are utilized over public networks for encrypting sensitive information to ensure the privacy and integrity of the data passing over the public network.	Inspected the site to site VPN encryption configurations and conducted a corroborative inquiry of management to determine that the connections were in place and utilized for the secure transmission of data.	No Exceptions Noted
	Remote user VPN connections are utilized by staff to establish encrypted communication sessions utilizing multi-factor authentication to the corporate network.	Inspected the VPN multi-factor authentication and encryption configuration to determine that the connections were in place and utilized by staff for establishing encrypted communication sessions to the corporate network.	No Exceptions Noted

## Trust Services Principle – Common Criteria (Continued)

*Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC6.0 Common Criteria Related to Logical and Physical Access Controls (Continued)			
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	LNRS has a Bring Your Own Device policy to establish governance on the use of personal non-company owned digital devices accessing LNRS infrastructure and its resources requiring standards for encryption and data protection of the device.	Inspected the Bring Your Own Device Policy and conducted a corroborative inquiry of management to determine that LNRS had a Bring Your Own Device to establish governance on the use of personal non-company owned digital devices accessing LNRS infrastructure and its resources requiring standards for encryption and data protection of the device.	No Exceptions Noted
	LNRS filters web site access through a network based URL filtering system to block non corporate approved web sites.	Inspected the web filtering configuration and conducted a corroborative inquiry of management to determine that LNRS filtered web site access through a proxy server to block non corporate approved web sites.	No Exceptions Noted
	LNRS blocks access to external personal e-mail systems.	Inspected the webmail restriction configuration and conducted a corroborative inquiry of management to determine that LNRS blocked access to external personal e-mail systems.	No Exceptions Noted
	LNRS blocks access to certain external instant messaging systems.	Inspected the instant messaging restriction configuration and conducted a corroborative inquiry of management to determine that LNRS blocked access to external instant messaging systems.	No Exceptions Noted
	Encrypted VPNs are utilized for remote access for the security and integrity of the data passing over the public network.	Inspected the site to site and remote user VPN settings and conducted a corroborative inquiry of management to determine that VPNs are in use.	No Exceptions Noted

## Trust Services Principle – Common Criteria (Continued)

*Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC6.0	Common Criteria Related to Logical and Physical Access Controls (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	Site to site VPN connections are utilized over public networks for encrypting sensitive information to ensure the privacy and integrity of the data passing over the public network.	Inspected the site to site VPN encryption configurations and conducted a corroborative inquiry of management to determine that the connections were in place and utilized for the secure transmission of data.	No Exceptions Noted
	Remote user VPN connections are utilized by staff to establish encrypted communication sessions utilizing multi-factor authentication to the corporate network.	Inspected the VPN multi-factor authentication and encryption configuration to determine that the connections were in place and utilized by staff for establishing encrypted communication sessions to the corporate network.	No Exceptions Noted
	SFTP / FTPs servers are utilized for encrypted file transfers and is monitored and administered by the IT department.	Inspected the SFTP server configurations and conducted a corroborative inquiry of management to determine that the server was being utilized as described.	No Exceptions Noted
	Secure communication tunnels are in place for interactive web sites and file transfers requiring encryption to LNRS' servers through the use of SSL/TLS encryption.	Inspected the web server encryption certificates and conducted a corroborative inquiry of management to determine that the server was being utilized as described.	No Exceptions Noted
	Encryption is in place for files sent via e-mail containing sensitive information.	Inspected an example encrypted email message and conducted a corroborative inquiry of management to determine that encryption was available.	No Exceptions Noted



**Trust Services Principle – Common Criteria (Continued)***Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC6.0 Common Criteria Related to Logical and Physical Access Controls (Continued)			
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	Management requires disk level encryption for laptops, portable devices and media.	Inspected the disk level encryption for the sampled laptops and conducted a corroborative inquiry of management to determine that management required disk level encryption for laptops, portable devices and media.	No Exceptions Noted
	Management controls the use of portable storage devices used for LNRS' business.	Inspected the centralized configuration preventing the use of portable storage devices and conducted a corroborative inquiry of management to determine that management prohibited the use of portable storage devices are controlled.	No Exceptions Noted
	Outbound connections to the internet are authenticated by a proxy device requiring proper credentials to access external resources.	Inspected the outbound connection firewall logs and conducted a corroborative inquiry of management to determine that outbound connections to the internet were authenticated by a proxy device requiring proper credentials to access external resources.	No Exceptions Noted
	Concurrent wireless and wired connections for purposes of connection sharing are prohibited.	Inspected the configurations that prevent concurrent connections and conducted a corroborative inquiry of management to determine that concurrent wireless and wired connections for purposes of connection sharing were prohibited.	No Exceptions Noted
	LNRS has implemented countermeasures to protect against denial of service attacks.	Inspected the DDoS Mitigation Procedure document to determine LNRS had implemented procedures and countermeasures to protect against denial of service attacks.	No Exceptions Noted



**Trust Services Principle – Common Criteria (Continued)***Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC6.0	Common Criteria Related to Logical and Physical Access Controls (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	Inbound traffic at perimeter networks and subnets containing confidential data is denied unless explicitly allowed.	Inspected the default deny firewall rule configuration to determine inbound traffic at perimeter networks and subnets containing confidential data is denied unless explicitly allowed.	No Exceptions Noted
	Stateful packet inspection is enabled on the firewall.	Inspected the stateful packet inspection configuration to determine stateful packet inspection is enabled on the firewall.	No Exceptions Noted
	Data Loss Prevention (DLP) software is configured on the LNRS network and workstations to prevent the unauthorized disclosure of sensitive information.	Inspected the DLP configuration at the network level and for the sampled workstations to determine Data Loss Prevention software is configured on the LNRS network and workstations to prevent the unauthorized disclosure of sensitive information.	No Exceptions Noted

## Trust Services Principle – Common Criteria (Continued)

*Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC6.0	Common Criteria Related to Logical and Physical Access Controls (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	Antivirus software is present on production servers and workstations and conducts regular system scans.	Inspected the antivirus configuration for the sampled workstations and servers to determine that countermeasures have been established and implemented to detect and remove malicious code.	No Exceptions Noted
	Antivirus software is configured to automatically update servers and personal computers on a daily basis.	Inspected the centralized antivirus update configurations to determine antivirus software was configured to automatically update servers and workstations.	No Exceptions Noted
	An Intrusion Prevention Systems (IPS) is utilized to continuously monitor the network for malicious activity and unauthorized access attempts.	Inspected the IPS configuration, the log history, and conducted a corroborative inquiry of management to determine that a IPS was in place, monitoring the network continuously, and provided alert to administrators.	No Exceptions Noted
	LNRS maintains an approved whitelist of allowed software.	Inspected the approved software catalog to determine it was in place as described and current.	No Exceptions Noted
	File-integrity monitoring (FIM) software is configured to detect and log modifications to critical system and application files.	Inspected the integrity log monitoring for the sampled servers to determine that File-integrity monitoring software was configured to alert operations personnel to unauthorized modifications to critical system files and databases.	No Exceptions Noted

**Trust Services Principle – Common Criteria (Continued)***Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC6.0	Common Criteria Related to Logical and Physical Access Controls (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	Patches are tested in lower environments by personnel prior to implementation into production.	Inspected the patch maintenance tracking tickets throughout the period to determine that patches were tested in lower environments by personnel prior to implementation into production.	No Exceptions Noted
	A Software Installation Policy is in place to provide guidance on the requirements of software installation on devices connecting to the Corporate network.	Inspected the Software Asset Management Standards and Procedures to determine that LNRS had a Software Installation Policy to provide guidance on the requirements of software installation on devices connecting to the Corporate network.	No Exceptions Noted
	A third party application is used to monitor network devices and generate e-mail notifications when certain events occur. Logs are analyzed either manually or by automated tools to identify trends that may have a potential impact on LNRS' ability to achieve its system security objectives.	Inspected the monitoring applications and alerting configurations and conducted a corroborative inquiry of management to determine that the third-party application generated notifications when certain network device events occurred.	No Exceptions Noted

## Trust Services Principle – Common Criteria (Continued)

*Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC7.0	Common Criteria Related to System Operations		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC7.1	To meet its objectives, as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.		
	A monitoring application is utilized to monitor network devices and critical systems.	Inspected the monitoring tools dashboards and available reports to determine that the organization utilized monitoring applications to measure production systems utilization and availability.	No Exceptions Noted
	Monitoring applications send e-mail alert notifications to operations personnel when predefined thresholds are exceeded on monitored network devices.	Inspected the samples of email alert notifications to determine that sufficient notification takes place when predefined thresholds are exceeded.	No Exceptions Noted
	Build procedures are documented and testing is performed when new systems are deployed to ensure hardware and operating systems are configured in accordance with LNRS' policies.	Inspected the network device and server build standards to determine that build guidelines and hardening procedures are followed and documented.	No Exceptions Noted
	A third party application is used to monitor network devices and generate e-mail notifications when certain events occur. Logs are analyzed either manually or by automated tools to identify trends that may have a potential impact on LNRS' ability to achieve its system security objectives.	Inspected the monitoring applications and alerting configurations and conducted a corroborative inquiry of management to determine that the third-party application generated notifications when certain network device events occurred.	No Exceptions Noted

**Trust Services Principle – Common Criteria (Continued)***Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC7.0 Common Criteria Related to System Operations			
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC7.1	To meet its objectives, as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.		
	Documented standards are in place and followed for the proper maintenance and operation of firewalls used on perimeter networks.	Inspected the Secure Firewall Procedures and Infrastructure Security Architecture and conducted a corroborative inquiry of management to determine that documented standards were in place and followed for the proper maintenance and operation of firewalls used on perimeter networks.	No Exceptions Noted
	Policies and procedures are in place for patch management on production systems.	Inspected the patch history for the sampled servers to determine that a patch management process was in place.	No Exceptions Noted
	File-integrity monitoring (FIM) software is configured to detect and log modifications to critical system and application files.	Inspected the integrity log monitoring for the sampled servers to determine that File-integrity monitoring software was configured to alert operations personnel to unauthorized modifications to critical system files and databases.	No Exceptions Noted
	LNRS subscribes to security bulletins and notices for newly discovered vulnerabilities in order to identify patches to be applied.	Inspected the example security bulletins from third party specialists and conducted a corroborative inquiry of management to determine that LNRS subscribed to security bulletins and notices for newly discovered vulnerabilities in order to identify patches to be applied.	No Exceptions Noted

**Trust Services Principle – Common Criteria (Continued)***Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC7.0 Common Criteria Related to System Operations			
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC7.1	To meet its objectives, as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.		
	The clocks of all relevant information processing systems within LNRS are synchronized with an accurate time source.	Inspected the time sync configuration for the selected servers and conducted a corroborative inquiry of management to determine that the system clocks of all relevant information processing systems within LNRS were synchronized with an accurate time source.	No Exceptions Noted
	An application is used to identify authorized and unauthorized devices connecting to the network.	Inspected the rogue access scans and the new device reporting functionality to determine that LNRS had automated applications to identify authorized and unauthorized devices connecting to the network.	No Exceptions Noted
	Vulnerability assessments are performed by a third-party vendor periodically to test for known vulnerabilities on the network and production systems.	Inspected the third-party vulnerability assessment reports and conducted a corroborative inquiry of management to determine whether the assessments were performed as described.	No Exceptions Noted
	Vulnerability scans are performed on an ongoing basis by IT staff to test for known vulnerabilities on the network and production systems to facilitate scheduled reporting to stakeholders.	Inspected the vulnerability scanning logs for the sampled months and conducted a corroborative inquiry of management to determine the assessments were performed as described.	No Exceptions Noted

## Trust Services Principle – Common Criteria (Continued)

*Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC7.0	Common Criteria Related to System Operations (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	Monitoring applications send e-mail alert notifications to operations personnel when predefined thresholds are exceeded on monitored network devices.	Inspected the samples of email alert notifications to determine that sufficient notification takes place when predefined thresholds are exceeded.	No Exceptions Noted
	LNRS has a Security Incident Response Policy and Procedures in place to provide policy guidance and establish responsibilities for responding to and reporting security breaches.	Inspected the Data Security Incident Response Overview and Incident Response and Notification Policy to determine that LNRS had a Security Incident Response Policy and Procedures in place to provide policy guidance for responding to and reporting security breaches.	No Exceptions Noted
	Status reports from the enterprise monitoring applications can be generated for adhoc review.	Inspected the monitoring tool dashboards and filtering functionality to determine that status reports were available for adhoc review.	No Exceptions Noted
	The access control system has the ability to generate entry and exit reports for review as necessary.	Inspected example entry reports to determine that the access control system can generate entry and exit reports for ad hoc review.	No Exceptions Noted
	Backup jobs are monitored and notification alerts are sent in the event of backup failure.	Inspected the backup alerting configurations, the example alerts, and conducted a corroborative inquiry of management to determine that alerts are sent in the event of backup failure.	No Exceptions Noted

**Trust Services Principle – Common Criteria (Continued)***Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC7.0 Common Criteria Related to System Operations (Continued)			
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	Network security event logging is configured to log specific events on the network domain.	Inspected the security event logging configuration and conducted a corroborative inquiry of management to determine that network audit settings were configured to log specific logon events on the domain.	No Exceptions Noted
	The firewall is configured to generate e-mail notifications when certain firewall events occur.	Inspected the firewall email alerts and conducted a corroborative inquiry of management to determine that it was configured to send notifications to administrators when certain events occurred.	No Exceptions Noted
	A third party application is used to monitor network devices and generate e-mail notifications when certain events occur. Logs are analyzed either manually or by automated tools to identify trends that may have a potential impact on LNRS' ability to achieve its system security objectives.	Inspected the monitoring applications and alerting configurations and conducted a corroborative inquiry of management to determine that the third-party application generated notifications when certain network device events occurred.	No Exceptions Noted
	An Intrusion Prevention Systems (IPS) is utilized to continuously monitor the network for malicious activity and unauthorized access attempts.	Inspected the IPS configuration, the log history, and conducted a corroborative inquiry of management to determine that a IPS was in place, monitoring the network continuously, and provided alert to administrators.	No Exceptions Noted



## Trust Services Principle – Common Criteria (Continued)

*Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC7.0 Common Criteria Related to System Operations (Continued)			
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	LNRS has a Security Incident Response Policy and Procedures in place to provide policy guidance and establish responsibilities for responding to and reporting security breaches.	Inspected the Data Security Incident Response Overview and Incident Response and Notification Policy to determine that LNRS had a Security Incident Response Policy and Procedures in place to provide policy guidance for responding to and reporting security breaches.	No Exceptions Noted
	The Incident Response Procedures require that all security events (actual or suspected) be reported to appropriate management personnel.	Inspected the Security Incident Response Overview to determine that the Incident Response Procedures required that all security events (actual or suspected) be reported to appropriate management personnel.	No Exceptions Noted
	The Incident Response Procedures require that all security events (actual or suspected) be assessed and classified, a documented response ticket is created as evidence of the assessment.	Inspected the Incident Response procedural documents to determine that the Incident Response Procedures required that all security events (actual or suspected) be assessed and classified, a documented response ticket was created as evidence of the assessment.	No Exceptions Noted
	The Incident Response Procedures require that all security events (actual or suspected) be assessed and classified, a review is conducted at the end of the process to identify any required changes to documented procedures.	Inspected the Incident Response procedures documents to determine that the Incident Response Procedures required that all security events (actual or suspected) be assessed and classified, a review was conducted at the end of the process to identify any required changes to documented procedures.	No Exceptions Noted

**Trust Services Principle – Common Criteria (Continued)***Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC7.0 Common Criteria Related to System Operations (Continued)			
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	The Incident Response Procedures documents the required procedures for evidence collection.	Inspected the Incident Response procedural documents to determine that the Incident Response Procedures documented the required procedures for evidence collection.	No Exceptions Noted
	A third party application is used to monitor network devices and generate e-mail notifications when certain events occur. Logs are analyzed either manually or by automated tools to identify trends that may have a potential impact on LNRS' ability to achieve its system security objectives.	Inspected the monitoring applications and alerting configurations and conducted a corroborative inquiry of management to determine that the third-party application generated notifications when certain network device events occurred.	No Exceptions Noted

**Trust Services Principle – Common Criteria (Continued)***Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC7.0	Common Criteria Related to System Operations (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC7.4	The entity responds to identified security incidents, as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy, by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.		
	LNRS has a Security Incident Response Policy and Procedures in place to provide policy guidance and establish responsibilities for responding to and reporting security breaches.	Inspected the Data Security Incident Response Overview and Incident Response and Notification Policy to determine that LNRS had a Security Incident Response Policy and Procedures in place to provide policy guidance for responding to and reporting security breaches.	No Exceptions Noted
	The Incident Response Procedures require that all security events (actual or suspected) be reported to appropriate management personnel.	Inspected the Security Incident Response Overview to determine that the Incident Response Procedures required that all security events (actual or suspected) be reported to appropriate management personnel.	No Exceptions Noted
	The Incident Response Procedures require that all security events (actual or suspected) be assessed and classified, a documented response ticket is created as evidence of the assessment.	Inspected the Incident Response procedural documents to determine that the Incident Response Procedures required that all security events (actual or suspected) be assessed and classified, a documented response ticket was created as evidence of the assessment.	No Exceptions Noted
	The Incident Response Procedures require that all security events (actual or suspected) be assessed and classified, a review is conducted at the end of the process to identify any required changes to documented procedures.	Inspected the Incident Response procedures documents to determine that the Incident Response Procedures required that all security events (actual or suspected) be assessed and classified, a review was conducted at the end of the process to identify any required changes to documented procedures.	No Exceptions Noted

**Trust Services Principle – Common Criteria (Continued)***Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC7.0 Common Criteria Related to System Operations (Continued)			
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC7.4	The entity responds to identified security incidents, as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy, by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.		
	The Incident Response Procedures documents the required procedures for evidence collection.	Inspected the Incident Response procedural documents to determine that the Incident Response Procedures documented the required procedures for evidence collection.	No Exceptions Noted
	There are formal discipline policies for employees who are suspected of rule infractions or violations of LNRS' policies.	Inspected the disciplinary process documents to determine that there was a formal policy for employees who were suspected of rule infractions or violations of LNRS' policies.	No Exceptions Noted

**Trust Services Principle – Common Criteria (Continued)***Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC7.0	Common Criteria Related to System Operations (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	Management maintains documented backup schedules, policies, and procedures.	Inspected the Data Backup Policy to determine that it was in place as described.	No Exceptions Noted
	Automated backup systems are utilized to perform the scheduled system backups of target data.	Inspected the automated backup configuration to determine that an automated backup system was utilized to perform the scheduled system backups.	No Exceptions Noted
	Backup jobs are monitored and notification alerts are sent in the event of backup failure.	Inspected the backup alerting configurations, the example alerts, and conducted a corroborative inquiry of management to determine that alerts are sent in the event of backup failure.	No Exceptions Noted
	Backup media containing target data utilizes password protected encryption to prevent unauthorized access.	Inspected the backup encryption configurations and conducted a corroborative inquiry of management to determine that backup media and backup sets were encrypted and password protected to restrict access.	No Exceptions Noted
	Restores from backups can be performed to verify that system components can be recovered from backup media.	Inspected the restore testing ticket to determine that restores from backups were performed to verify that system components can be recovered from backup media.	No Exceptions Noted
	Access to modify backup jobs and backup job notification settings is restricted to authorized personnel.	Inspected the authorized backup administrators and conducted a corroborative inquiry of management to determine that access to make changes to the backup jobs and backup notification settings was restricted to authorized personnel.	No Exceptions Noted

## Trust Services Principle – Common Criteria (Continued)

*Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC7.0	Common Criteria Related to System Operations (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	LNRS has a Security Incident Response Policy and Procedures in place to provide policy guidance and establish responsibilities for responding to and reporting security breaches.	Inspected the Data Security Incident Response Overview and Incident Response and Notification Policy to determine that LNRS had a Security Incident Response Policy and Procedures in place to provide policy guidance for responding to and reporting security breaches.	No Exceptions Noted
	The Incident Response Procedures require that all security events (actual or suspected) be assessed and classified, a documented response ticket is created as evidence of the assessment.	Inspected the Incident Response procedural documents to determine that the Incident Response Procedures required that all security events (actual or suspected) be assessed and classified, a documented response ticket was created as evidence of the assessment.	No Exceptions Noted
	Management maintains a disaster recovery plan (DRP) to facilitate disaster recovery operations.	Inspected the Technical Resilience Program, the Business Continuity Management Policy, and conducted a corroborative inquiry of management to determine that it was in place to facilitate disaster recovery operations.	No Exceptions Noted
	The disaster recovery plan is reviewed by management on an annual basis and revised as necessary.	Inspected the Technical Resilience Program and Business Continuity Management Policy revision dates and conducted a corroborative inquiry of management to determine that it was revised annually.	No Exceptions Noted

## Trust Services Principle – Common Criteria (Continued)

*Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC7.0 Common Criteria Related to System Operations (Continued)			
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	Certain aspects of the disaster recovery plan are tested on an annual basis.	Inspected the Disaster Recovery and Technical Resiliency testing summary reports and conducted a corroborative inquiry of management to determine that certain aspects of the disaster recovery plan were tested within the last 12 months.	No Exceptions Noted
	LNRS has documented a formal Business Continuity Program which outlines the following components: the goals, objectives, and internal/external obligations of the BC Program; the scope of products and services included in the BC Program and the relevant exclusions; the relevant internal and external parties and their requirements including what types of information to be communicated, when, and how; the internal and external issues affecting the ability of LNRS to achieve the intended outcomes of the BC Program; and the process for identifying and addressing applicable legal, regulatory, and contractual requirements related to business continuity.	Inspected the documented Technical Resiliency Programs for a subset of products and services and conducted corroborative inquiry with management to determine LNRS had documented business continuity programs as described.	No Exceptions Noted
	LNRS' Business Continuity Program and Disaster Recovery Program are available to internal users who need access via LNRS' SharePoint.	Inspected the internal availability of documentation on LNRS' SharePoint to determine LNRS' Business Continuity Program and Disaster Recovery Program are available to internal users who need access via LNRS' SharePoint.	No Exceptions Noted

## Trust Services Principle – Common Criteria (Continued)

*Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC7.0	Common Criteria Related to System Operations (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	LNRS assesses the risks that it's business continuity program will not meet its objectives or achieve its intended outcomes.	Inspected the risk assessment documentation to determine LNRS assesses the risks that it's business continuity program will not meet its objectives or achieve its intended outcomes.	No Exceptions Noted
	Changes to the Business Continuity Program are formally evaluated and tested to ensure the continued availability of resources and the appropriate assignment of responsibilities.	Inspected the technical resiliency testing documentation to determine changes to the Business Continuity Program are formally evaluated and tested to ensure the continued availability of resources and the appropriate assignment of responsibilities.	No Exceptions Noted
	LNRS evaluates potential business impacts to define business continuity activity prioritization, resource dependencies, and recovery time objectives/requirements.	Inspected the Business Impact Analysis procedures as included in the Technical Resiliency Program documentation to determine LNRS evaluates potential business impacts to define business continuity activity prioritization, resource dependencies, and recovery time objectives/requirements.	No Exceptions Noted
	The Business Continuity and Technical Recovery Programs define the roles and responsibilities for the assigned teams, the interdependencies of resources and teams, and the alternate/backups for the primary personnel and resources.	Inspected the defined key personnel and roles as included in the Technical Resiliency program documentation to determine LNRS evaluates potential business impacts to define business continuity activity prioritization, resource dependencies, and recovery time objectives/requirements.	No Exceptions Noted



**Trust Services Principle – Common Criteria (Continued)***Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC7.0	Common Criteria Related to System Operations (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	LNRS' Business Continuity Program includes testing the procedures to transition back to normal operating conditions from the temporary measures adopted during and after a disruption.	Inspected the technical resiliency testing reports to determine LNRS' Business Continuity Program includes testing the procedures to transition back to normal operating conditions from the temporary measures adopted during and after a disruption.	No Exceptions Noted
	For nonconformities that occurred during the period under review, LNRS takes appropriate action to rectify the conformity, evaluate the cause of the nonconformity, implement corrective action plans to prevent future nonconformities, and if necessary, modify the BCP.	Inspected the technical resiliency plan reviews and testing documentation to determine nonconformities identified in the BCP testing are identified and recommended action items are documented to improve upon the BCP.	No Exceptions Noted

## Trust Services Principle – Common Criteria (Continued)

*Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC8.0 Common Criteria Related to Change Management			
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	LNRS' application program code is designed and documented in accordance with written standards and procedures established by management in the SDLC.	Inspected the Secure Software Development Lifecycle Standards and conducted a corroborative inquiry of management to determine that the phases of the systems development and maintenance processes were documented.	No Exceptions Noted
	A tracking system is used to log critical and non-critical application change requests (issues/projects) reported by users or internal parties.	Inspected the change ticketing tracking system and conducted a corroborative inquiry of management to determine that a ticketing system was used.	No Exceptions Noted
	Separate environments exist for development, testing, and production to prevent making changes that would affect the performance, availability, and integrity of production application code.	Inspected the separate source code environments, the rules for merging changes between environments, and conducted a corroborative inquiry of management to determine they were logically separated.	No Exceptions Noted
	Build procedures are documented and testing is performed when new systems are deployed to ensure hardware and operating systems are configured in accordance with LNRS' policies.	Inspected the network device and server build standards to determine that build guidelines and hardening procedures are followed and documented.	No Exceptions Noted
	QA testing is documented and performed for development and maintenance activities prior to production release.	Inspected the QA reviews for the sample selected software application releases and conducted a corroborative inquiry of management to determine that QA testing was performed for development and maintenance activities.	No Exceptions Noted

**Trust Services Principle – Common Criteria (Continued)***Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC8.0	Common Criteria Related to Change Management		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	Development projects a reviewed and approved by management prior to implementation into the production environment.	Inspected the approvals for the sampled changes and conducted a corroborative inquiry of management to determine that development projects were subjected to management review and approval prior to implementation into the production environment.	No Exceptions Noted
	The Development team has adopted OWASP-based standards for building, designing, and testing the security of web applications and web services.	Inspected the SDLC Policy and the Baselines Application Security Requirements and conducted a corroborative inquiry of management to determine to determine that OWASP Top 10 testing was performed for development and maintenance activities.	No Exceptions Noted
	Rollback procedures are defined for production changes when applicable.	Inspected the rollback procedure for the sampled changes to determine rollback procedures are defined for production changes when applicable.	No Exceptions Noted
	Patches are tested in lower environments by personnel prior to implementation into production.	Inspected the patch maintenance tracking tickets throughout the period to determine that patches were tested in lower environments by personnel prior to implementation into production.	No Exceptions Noted

## Trust Services Principle – Common Criteria (Continued)

*Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC8.0	Common Criteria Related to Change Management		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	Policies and procedures are in place to guide personnel on their responsibility for the handling of client information related to the secure storage and destruction of sensitive data and documents.	Inspected the Records Management Policy, the Information Value Classification Procedures, and conducted a corroborative inquiry of management to determine that policies were in place to guide personnel on their responsibility for the handling of client information related to the secure storage and destruction of sensitive data and documents.	No Exceptions Noted
	An Infrastructure Change Management Policy is in place to guide personnel on documenting and implementing change control procedures that affect production systems.	Inspected the Change Management Standard and conducted a corroborative inquiry of management to determine policies were in place to guide changes made to infrastructure.	No Exceptions Noted
	Changes to the production environment are documented in the ticketing system and a work order is created.	Inspected the tickets for a sample of infrastructure changes and firewall changes and conducted a corroborative inquiry of management to determine that changes were logged in a ticketing system.	No Exceptions Noted
	The Change review board or IT Management must approve proposed changes that affect the production environment.	Inspected the tickets for a sample of infrastructure changes and firewall and conducted a corroborative inquiry of management to determine that changes were properly reviewed and approved.	No Exceptions Noted

## Trust Services Principle – Common Criteria (Continued)

*Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC8.0	Common Criteria Related to Change Management		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	Changes are tested and configured prior to production deployment.	Inspected the tickets for a sample of infrastructure changes and firewall and conducted a corroborative inquiry of management to determine a successful test process.	No Exceptions Noted
	Changes are authorized and scheduled when testing is complete.	Inspected the tickets for a sample of infrastructure changes and firewall and conducted a corroborative inquiry of management to determine that changes were authorized and scheduled when testing was complete.	No Exceptions Noted
	Escalation procedures are in place to assign tickets to technical or application personnel that required an elevated level of support.	Inspected the escalation process and conducted a corroborative inquiry of management to determine that tickets followed escalation procedures when required by the nature of the issue.	No Exceptions Noted
	Production data utilized in non-production environments is truncated/masked for confidentiality or is generated randomly.	Inspected the Appropriate Use of Data in Non-Production Environments Standard to determine production data utilized in non-production environments is truncated/masked for confidentiality or is generated randomly.	No Exceptions Noted
	A Security Framework is defined and met regarding network architecture to ensure adherence to security policies, objectives and standards.	Inspected the Infrastructure Security Architecture standards to determine that a Security Framework is defined and met regarding network architecture to ensure adherence to security policies, objectives and standards.	No Exceptions Noted

## Trust Services Principle – Common Criteria (Continued)

*Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC9.0 Common Criteria Related to Risk Mitigation			
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	LNRS maintains insurance policies to mitigate losses and transfer certain identified risks.	Inspected the insurance coverage forms to determine that LNRS maintained insurance policies to mitigate losses and transfer certain identified risks.	No Exceptions Noted
	LNRS requires all 3rd parties such as vendors and suppliers to sign contracts which provides guidance on security requirements and responsibilities.	Inspected the signed agreements for the sampled vendors and conducted a corroborative inquiry of management to determine that LNRS required all 3rd parties such as vendors and suppliers to acknowledge the information security policy which provided governance on connections to corporate resources.	No Exceptions Noted
	LNRS completes a risk assessment and updates the list of identified risks periodically.	Inspected the risk assessment spreadsheets to determine that LNRS completed a risk assessment and updated the identified risks.	No Exceptions Noted
	LNRS assesses the risks that vendors and business partners will fail to meet LNRS's requirements.	Inspected the third-party risk considerations to determine that LNRS assessed the risks that vendors and business partners will fail to meet LNRS's requirements.	No Exceptions Noted
	LNRS considers fraud when completing its risk assessment.	Inspected the fraud considerations in the risk assessment to determine that LNRS included fraud within their risk assessment.	No Exceptions Noted

## Trust Services Principle – Common Criteria (Continued)

*Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC9.0	Common Criteria Related to Risk Mitigation		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	Management maintains a disaster recovery plan (DRP) to facilitate disaster recovery operations.	Inspected the Technical Resilience Program, the Business Continuity Management Policy, and conducted a corroborative inquiry of management to determine that it was in place to facilitate disaster recovery operations.	No Exceptions Noted
	The disaster recovery plan is reviewed by management on an annual basis and revised as necessary.	Inspected the Technical Resilience Program and Business Continuity Management Policy revision dates and conducted a corroborative inquiry of management to determine that it was revised annually.	No Exceptions Noted
	Certain aspects of the disaster recovery plan are tested on an annual basis.	Inspected the Disaster Recovery and Technical Resiliency testing summary reports and conducted a corroborative inquiry of management to determine that certain aspects of the disaster recovery plan were tested within the last 12 months.	No Exceptions Noted
	Management maintains documented backup schedules, policies, and procedures.	Inspected the Data Backup Policy to determine that it was in place as described.	No Exceptions Noted
	Automated backup systems are utilized to perform the scheduled system backups of target data.	Inspected the automated backup configuration to determine that an automated backup system was utilized to perform the scheduled system backups.	No Exceptions Noted
	Backup jobs are monitored and notification alerts are sent in the event of backup failure.	Inspected the backup alerting configurations, the example alerts, and conducted a corroborative inquiry of management to determine that alerts are sent in the event of backup failure.	No Exceptions Noted

**Trust Services Principle – Common Criteria (Continued)***Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC9.0	Common Criteria Related to Risk Mitigation		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	Backup media containing target data utilizes password protected encryption to prevent unauthorized access.	Inspected the backup encryption configurations and conducted a corroborative inquiry of management to determine that backup media and backup sets were encrypted and password protected to restrict access.	No Exceptions Noted
	Restores from backups can be performed to verify that system components can be recovered from backup media.	Inspected the restore testing ticket to determine that restores from backups were performed to verify that system components can be recovered from backup media.	No Exceptions Noted
	Vulnerability assessments are performed by a third-party vendor periodically to assess vulnerabilities to the network and production systems.	Inspected the vulnerability scanning and penetration testing reports to determine vulnerability assessments are performed by a third-party vendor periodically to assess vulnerabilities to the network and production systems.	No Exceptions Noted
	Network Penetration tests are performed by IT staff periodically to gain unauthorized access to the network and production systems.	Inspected the penetration testing reports to determine network penetration tests are performed by IT staff periodically to gain unauthorized access to the network and production systems.	No Exceptions Noted



## Trust Services Principle – Common Criteria (Continued)

*Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC9.0	Common Criteria Related to Risk Mitigation		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	LNRS has documented a formal Business Continuity Program which outlines the following components: the goals, objectives, and internal/external obligations of the BC Program; the scope of products and services included in the BC Program and the relevant exclusions; the relevant internal and external parties and their requirements including what types of information to be communicated, when, and how; the internal and external issues affecting the ability of LNRS to achieve the intended outcomes of the BC Program; and the process for identifying and addressing applicable legal, regulatory, and contractual requirements related to business continuity.	Inspected the documented Technical Resiliency Programs for a subset of products and services and conducted corroborative inquiry with management to determine LNRS had documented business continuity programs as described.	No Exceptions Noted
	LNRS' Business Continuity Program and Disaster Recovery Program are available to internal users who need access via LNRS' SharePoint.	Inspected the internal availability of documentation on LNRS' SharePoint to determine LNRS' Business Continuity Program and Disaster Recovery Program are available to internal users who need access via LNRS' SharePoint.	No Exceptions Noted
	LNRS assesses the risks that it's business continuity program will not meet its objectives or achieve its intended outcomes.	Inspected the risk assessment documentation to determine LNRS assesses the risks that it's business continuity program will not meet its objectives or achieve its intended outcomes.	No Exceptions Noted

**Trust Services Principle – Common Criteria (Continued)***Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC9.0	Common Criteria Related to Risk Mitigation		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	Changes to the Business Continuity Program are formally evaluated and tested to ensure the continued availability of resources and the appropriate assignment of responsibilities.	Inspected the technical resiliency testing documentation to determine changes to the Business Continuity Program are formally evaluated and tested to ensure the continued availability of resources and the appropriate assignment of responsibilities.	No Exceptions Noted
	LNRS evaluates potential business impacts to define business continuity activity prioritization, resource dependencies, and recovery time objectives/requirements.	Inspected the Business Impact Analysis procedures as included in the Technical Resiliency Program documentation to determine LNRS evaluates potential business impacts to define business continuity activity prioritization, resource dependencies, and recovery time objectives/requirements.	No Exceptions Noted
	The Business Continuity and Technical Recovery Programs define the roles and responsibilities for the assigned teams, the interdependencies of resources and teams, and the alternate/backups for the primary personnel and resources.	Inspected the defined key personnel and roles as included in the Technical Resiliency program documentation to determine LNRS evaluates potential business impacts to define business continuity activity prioritization, resource dependencies, and recovery time objectives/requirements.	No Exceptions Noted

**Trust Services Principle – Common Criteria (Continued)***Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC9.0	Common Criteria Related to Risk Mitigation		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	LNRS' Business Continuity Program includes testing the procedures to transition back to normal operating conditions from the temporary measures adopted during and after a disruption.	Inspected the technical resiliency testing reports to determine LNRS' Business Continuity Program includes testing the procedures to transition back to normal operating conditions from the temporary measures adopted during and after a disruption.	No Exceptions Noted
	For nonconformities that occurred during the period under review, LNRS takes appropriate action to rectify the conformity, evaluate the cause of the nonconformity, implement corrective action plans to prevent future nonconformities, and if necessary, modify the BCP.	Inspected the technical resiliency plan reviews and testing documentation to determine nonconformities identified in the BCP testing are identified and recommended action items are documented to improve upon the BCP.	No Exceptions Noted

**Trust Services Principle – Common Criteria (Continued)***Common Criteria to Security, Availability, Confidentiality, Processing Integrity, and Privacy.*

CC9.0	Common Criteria Related to Risk Mitigation (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
CC9.2	The entity assesses and manages risks associated with vendors and business partners as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.		
	A Policy is in place to review and monitor the ongoing performance of the sub-service organizations.	Inspected the Third Parties Security Policy to determine that a Policy was in place to review and monitor the ongoing performance of the sub-service organizations.	No Exceptions Noted
	LNRS conducts periodic vendor assessments (based on vendor classification) to evaluate assessment results and review any 3 <sup>rd</sup> party assessments on contracted subservice organizations and vendors.	Inspected the vendor review assessments for the sample selected vendors to determine that LNRS has documented procedures for onboarding new vendors.	Exceptions Noted, See Below
	One (1) of the eighteen (18) sampled vendors did not have a review conducted in a timely manner.		
	LNRS assesses the risks that vendors and business partners will fail to meet LNRS's requirements.	Inspected the third-party risk considerations to determine that LNRS assessed the risks that vendors and business partners will fail to meet LNRS's requirements.	No Exceptions Noted

## Trust Services Principle – Availability

*The system is available to users as committed or agreed.*

A1.0	Additional criteria related to availability		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.		
	A monitoring application is utilized to monitor network devices and critical systems.	Inspected the monitoring tools dashboards and available reports to determine that the organization utilized monitoring applications to measure production systems utilization and availability.	No Exceptions Noted
	Monitoring applications send e-mail alert notifications to operations personnel when predefined thresholds are exceeded on monitored network devices.	Inspected the samples of email alert notifications to determine that sufficient notification takes place when predefined thresholds are exceeded.	No Exceptions Noted
	LNRS has established load balancing on certain systems to ensure high availability and a responsive end user experience.	Inspected the configured load balancing server pools to determine that load balancing had been implemented to ensure high availability and a pleasant end-user experience.	No Exceptions Noted

**Trust Services Principle – Availability (Continued)***The system is available to users as committed or agreed.*

A1.0	Additional criteria related to availability (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.		
	The data center is equipped with sensors to detect the presence of smoke and fire. Monitored by Onsite personnel.	Observed the fire detection systems during onsite procedures to determine that the data center was equipped with sensors to detect the presence of smoke and fire.	No Exceptions Noted
	The data center is equipped with a fixed fire suppression system.	Observed the fixed fire suppression system during onsite procedures to determine that the data center was equipped with a fixed fire suppression system.	No Exceptions Noted
	Periodic inspections of fire detection and suppression systems are conducted.	Inspected the fire suppression systems inspection reports to determine that periodic inspections of fire detection and suppression systems were conducted.	No Exceptions Noted
	The data center is equipped with HVAC systems used to control temperature and humidity.	Observed the HVAC systems during onsite procedures to determine that the data center was equipped with HVAC systems used to control temperature and humidity.	No Exceptions Noted
	The data center is equipped with backup HVAC systems should a failure occur to primary units.	Observed the redundant HVAC systems during onsite procedures to determine that the data center was equipped with backup HVAC systems should a failure occur to primary units.	No Exceptions Noted
	The data center has been configured with hot and cold aisles to maximize cooler airflow to the front of systems.	Observed the data center layout during onsite procedures to determine that the data center was configured with hot and cold aisles to maximize cooler airflow to the front of systems.	No Exceptions Noted

**Trust Services Principle – Availability (Continued)***The system is available to users as committed or agreed.*

A1.0	Additional criteria related to availability (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.		
	The data center utilizes monitoring devices that alert operations staff if the data center air temperature or humidity levels exceed predetermined thresholds.	Inspected the monitoring devices and alerting configurations to determine that the data center utilized monitoring devices that alert operations staff if the data center air temperature or humidity levels exceed predetermined thresholds.	No Exceptions Noted
	Preventative maintenance inspections are performed periodically on HVAC systems.	Inspected the HVAC maintenance reports to determine that preventative maintenance inspections were performed periodically on HVAC systems.	No Exceptions Noted
	An Uninterruptible Power Supply (UPS) system is in place to provide alternate power in the event of a momentary interruption in commercial power.	Observed the UPS systems during onsite procedures to determine that a UPS system was in place to provide alternate power in the event of a momentary interruption in commercial power.	No Exceptions Noted
	The Uninterruptible Power Supply (UPS) systems are periodically inspected to ensure operating effectiveness.	Inspected the UPS inspection and maintenance reports to determine that the UPS systems were inspected periodically to ensure operating effectiveness.	No Exceptions Noted
	A generator is in place to provide power in the event of an extended power outage.	Observed the generator systems during onsite procedures to determine that a generator was in place to provide power in the event of an extended power outage.	No Exceptions Noted

## Trust Services Principle – Availability (Continued)

*The system is available to users as committed or agreed.*

A1.0	Additional criteria related to availability (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.		
	The generator is regularly maintained, inspected, and tested to ensure proper operation.	Inspected the generator maintenance reports to determine that the generator was regularly maintained, inspected, and tested to ensure proper operation.	No Exceptions Noted
	The data center has Power Distribution Units (PDUs) configured to control power to rack mounted and floor seated systems.	Observed the PDUs during onsite procedures to determine that the data center had PDUs configured to control power to rack mounted and floor seated systems.	No Exceptions Noted
	The data center is equipped with raised flooring to protect against static buildup and water leaks.	Observed the raised flooring during onsite procedures to determine that the data center was equipped with raised flooring.	No Exceptions Noted
	The raised flooring in the data center is grounded to reduce the occurrence of electrostatic buildup.	Observed the raised flooring during onsite procedures to determine that the raised flooring in the data center was grounded to reduce the occurrence of electrostatic buildup.	No Exceptions Noted
	The data center is equipped with water detection devices to prevent water damage in the event of a flood and/or water leak.	Observed the water sensors during onsite procedures to determine that the data center was equipped with water detection devices to prevent water damage in the event of a flood and/or water leak.	No Exceptions Noted
	Management maintains a disaster recovery plan (DRP) to facilitate disaster recovery operations.	Inspected the Technical Resilience Program, the Business Continuity Management Policy, and conducted a corroborative inquiry of management to determine that it was in place to facilitate disaster recovery operations.	No Exceptions Noted



**Trust Services Principle – Availability (Continued)***The system is available to users as committed or agreed.*

A1.0	Additional criteria related to availability (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.		
	LNRS maintains failover data centers in order to provide recovery services in the event of a disaster.	Observed the use of geographically dispersed failover data centers and conducted a corroborative inquiry of management to determine that LNRS maintains failover data centers in order to provide recovery services in the event of a disaster.	No Exceptions Noted
	Management maintains documented backup schedules, policies, and procedures.	Inspected the Data Backup Policy to determine that it was in place as described.	No Exceptions Noted
	Automated backup systems are utilized to perform the scheduled system backups of target data.	Inspected the automated backup configuration to determine that an automated backup system was utilized to perform the scheduled system backups.	No Exceptions Noted
	Backup jobs are monitored and notification alerts are sent in the event of backup failure.	Inspected the backup alerting configurations, the example alerts, and conducted a corroborative inquiry of management to determine that alerts are sent in the event of backup failure.	No Exceptions Noted
	Backup media containing target data utilizes password protected encryption to prevent unauthorized access.	Inspected the backup encryption configurations and conducted a corroborative inquiry of management to determine that backup media and backup sets were encrypted and password protected to restrict access.	No Exceptions Noted

## Trust Services Principle – Availability (Continued)

*The system is available to users as committed or agreed.*

A1.0	Additional criteria related to availability (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.		
	Access to modify backup jobs and backup job notification settings is restricted to authorized personnel.	Inspected the authorized backup administrators and conducted a corroborative inquiry of management to determine that access to make changes to the backup jobs and backup notification settings was restricted to authorized personnel.	No Exceptions Noted
	The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.	Observed the emergency lighting during onsite procedures to determine the organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.	No Exceptions Noted

**Trust Services Principle – Availability (Continued)***The system is available to users as committed or agreed.*

A1.0	Additional criteria related to availability (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.		
	Restores from backups can be performed to verify that system components can be recovered from backup media.	Inspected the restore testing ticket to determine that restores from backups were performed to verify that system components can be recovered from backup media.	No Exceptions Noted
	Certain aspects of the disaster recovery plan are tested on an annual basis.	Inspected the Disaster Recovery and Technical Resiliency testing summary reports and conducted a corroborative inquiry of management to determine that certain aspects of the disaster recovery plan were tested within the last 12 months.	No Exceptions Noted
	Changes to the Business Continuity Program are formally evaluated and tested to ensure the continued availability of resources and the appropriate assignment of responsibilities.	Inspected the technical resiliency testing documentation to determine changes to the Business Continuity Program are formally evaluated and tested to ensure the continued availability of resources and the appropriate assignment of responsibilities.	No Exceptions Noted
	LNRS evaluates potential business impacts to define business continuity activity prioritization, resource dependencies, and recovery time objectives/requirements.	Inspected the Business Impact Analysis procedures as included in the Technical Resiliency Program documentation to determine LNRS evaluates potential business impacts to define business continuity activity prioritization, resource dependencies, and recovery time objectives/requirements.	No Exceptions Noted

**Trust Services Principle – Availability (Continued)**  
*The system is available to users as committed or agreed*

A1.0	Additional criteria related to availability (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.		
	LNRS' Business Continuity Program includes testing the procedures to transition back to normal operating conditions from the temporary measures adopted during and after a disruption.	Inspected the technical resiliency testing reports to determine LNRS' Business Continuity Program includes testing the procedures to transition back to normal operating conditions from the temporary measures adopted during and after a disruption.	No Exceptions Noted
	For nonconformities that occurred during the period under review, LNRS takes appropriate action to rectify the conformity, evaluate the cause of the nonconformity, implement corrective action plans to prevent future nonconformities, and if necessary, modify the BCP.	Inspected the technical resiliency plan reviews and testing documentation to determine nonconformities identified in the BCP testing are identified and recommended action items are documented to improve upon the BCP.	No Exceptions Noted

## Trust Services Principle – Processing Integrity

*System processing is complete, valid, accurate, timely, and authorized.*

PI1.0	Additional controls related to Processing Integrity		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
PI1.1	The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services.		
	A description of the system is posted on LNRS' Public Web Site and is available to users.	Inspected LNRS' public website to determine a description of the system is posted on LNRS' Public Web Site and is available to users.	No Exceptions Noted
	Employees are aware of the limits existing for their use of the organization's information and assets associated with information processing facilities and resources; and they are responsible for their use of any information resource and of any use carried out under their responsibility.	Inspected the Internal Use of LexisNexis Restricted Information Products and Product Data Policy to determine a policy was in place to provide guidance on the use of the organization's information and assets associated with information processing facilities and resources.	No Exceptions Noted

## Trust Services Principle – Processing Integrity (Continued)

*System processing is complete, valid, accurate, timely, and authorized.*

PI1.0	Additional controls related to Processing Integrity (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
PI1.2	The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives.		
	LNRS has documented standard operating procedures to communicate the responsibilities and requirements in the operation of the system.	Inspected the example SOP documents and conducted corroborative inquiry of management to determine that standard operating procedures were documented and in place.	No Exceptions Noted
	The system will generate error reports or onscreen notifications if information is received that does not match the requirements of the Batch system.	Observed the error reports and notifications for a sample of failed batch transfers and conducted corroborative inquiry with management to determine the system will generate error reports or onscreen notifications if information is received that does not match the requirements of the Batch system.	No Exceptions Noted

**Trust Services Principle – Processing Integrity (Continued)***System processing is complete, valid, accurate, timely, and authorized.*

PI1.0	Additional controls related to Processing Integrity (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
PI1.3	The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity's objectives.		
	LNRS has documented standard operating procedures to communicate the responsibilities and requirements in the operation of the system.	Inspected the example SOP documents and conducted corroborative inquiry of management to determine that standard operating procedures were documented and in place.	No Exceptions Noted
	Management has documented support operations procedures to outline how customer reported issues are addressed and resolved.	Inspected the support documentation and conducted a corroborative inquiry of management to determine that they were in place and current.	No Exceptions Noted
	Escalation procedures are in place to assign tickets to technical or application personnel that required an elevated level of support.	Inspected the escalation process and conducted a corroborative inquiry of management to determine that tickets followed escalation procedures when required by the nature of the issue.	No Exceptions Noted
	Committed Service Level Agreement monitoring results are reviewed with applicable internal personnel on a monthly basis.	Inspected the SLA monitoring reports for several months throughout the audit period and conducted a corroborative inquiry of management to determine that committed Service Level Agreement monitoring results were reviewed with applicable internal personnel on a monthly basis.	No Exceptions Noted
	LNRS' application program code is designed and documented in accordance with written standards and procedures established by management in the SDLC.	Inspected the Secure Software Development Lifecycle Standards and conducted a corroborative inquiry of management to determine that the phases of the systems development and maintenance processes were documented.	No Exceptions Noted

## Trust Services Principle – Processing Integrity (Continued)

*System processing is complete, valid, accurate, timely, and authorized.*

PI1.0	Additional controls related to Processing Integrity (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
PI1.3	The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity's objectives.		
	Separate environments exist for development, testing, and production to prevent making changes that would affect the performance, availability, and integrity of production application code.	Inspected the separate source code environments, the rules for merging changes between environments, and conducted a corroborative inquiry of management to determine they were logically separated.	No Exceptions Noted
	QA testing is documented and performed for development and maintenance activities prior to production release.	Inspected the QA reviews for the sample selected software application releases and conducted a corroborative inquiry of management to determine that QA testing was performed for development and maintenance activities.	No Exceptions Noted
	Development projects are reviewed and approved by management prior to implementation into the production environment.	Inspected the approvals for the sampled changes and conducted a corroborative inquiry of management to determine that development projects were subjected to management review and approval prior to implementation into the production environment.	No Exceptions Noted
	The system will generate error reports or onscreen notifications if information is received that does not match the requirements of the Batch system.	Observed the error reports and notifications for a sample of failed batch transfers and conducted corroborative inquiry with management to determine the system will generate error reports or onscreen notifications if information is received that does not match the requirements of the Batch system.	No Exceptions Noted



## Trust Services Principle – Processing Integrity (Continued)

*System processing is complete, valid, accurate, timely, and authorized.*

PI1.0	Additional controls related to Processing Integrity (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
PI1.4	The entity implements policies and procedures to make available or deliver output completely, accurately, and timely in accordance with specifications to meet the entity's objectives.		
	LNRS has documented standard operating procedures to communicate the responsibilities and requirements in the operation of the system.	Inspected the example SOP documents and conducted corroborative inquiry of management to determine that standard operating procedures were documented and in place.	No Exceptions Noted
	Internal auditing of LNRS' processes is performed periodically.	Inspected the internal auditing schedules to determine that periodic internal auditing was performed.	No Exceptions Noted
	The system will generate error reports or onscreen notifications if information is received that does not match the requirements of the Batch system.	Observed the error reports and notifications for a sample of failed batch transfers and conducted corroborative inquiry with management to determine the system will generate error reports or onscreen notifications if information is received that does not match the requirements of the Batch system.	No Exceptions Noted
	The batch system has various dashboards and filtering functionality that are used to generate reports for adhoc review.	Observed the batch system filtering and reporting functionality to determine the batch system has various dashboards and filtering functionality that are used to generate reports for adhoc review.	No Exceptions Noted

## Trust Services Principle – Processing Integrity (Continued)

*System processing is complete, valid, accurate, timely, and authorized.*

PI1.0	Additional controls related to Processing Integrity (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
PI1.5	The entity implements policies and procedures to store inputs, items in processing, and outputs completely, accurately, and timely in accordance with system specifications to meet the entity's objectives.		
	Backup media containing target data utilizes password protected encryption to prevent unauthorized access.	Inspected the backup encryption configurations and conducted a corroborative inquiry of management to determine that backup media and backup sets were encrypted and password protected to restrict access.	No Exceptions Noted
	File-integrity monitoring (FIM) software is configured to detect and log modifications to critical system and application files.	Inspected the integrity log monitoring for the sampled servers to determine that File-integrity monitoring software was configured to alert operations personnel to unauthorized modifications to critical system files and databases.	No Exceptions Noted
	Administration rights to databases are restricted to only authorized personnel.	Inspected the authorized users for database access and conducted a corroborative inquiry of management to determine that access was restricted to only certain authorized administrators.	No Exceptions Noted
	Systems Logs and Audit Trails are restricted and protected from unauthorized access and deletion.	Inspected the restrictions on the ability to modify or purge logs and conducted a corroborative inquiry of management to determine that system logs and audit trails were protected from unauthorized access and deletion.	No Exceptions Noted
	Databases containing sensitive data are encrypted.	Inspected the database encryption configurations and conducted an inquiry of management to determine that databases containing sensitive data were encrypted.	No Exceptions Noted

## Trust Services Principle – Processing Integrity (Continued)

*System processing is complete, valid, accurate, timely, and authorized.*

PI1.0	Additional controls related to Processing Integrity (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
PI1.5	The entity implements policies and procedures to store inputs, items in processing, and outputs completely, accurately, and timely in accordance with system specifications to meet the entity's objectives.		
	Management requires disk level encryption for laptops, portable devices and media.	Inspected the disk level encryption for the sampled laptops and conducted a corroborative inquiry of management to determine that management required disk level encryption for laptops, portal devices and media.	No Exceptions Noted
	The batch system has various dashboards and filtering functionality that are used to generate reports for adhoc review.	Observed the batch system filtering and reporting functionality to determine the batch system has various dashboards and filtering functionality that are used to generate reports for adhoc review.	No Exceptions Noted

## Trust Services Principle – Confidentiality

*Information designated as confidential is protected as committed or agreed.*

C1.0	Additional criteria related to Confidentiality		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.		
	Employees must sign a confidentiality agreement as acknowledgment not to disclose proprietary or confidential information.	Inspected the confidentiality agreements for the sample selected new hire employees to determine that employees were required to sign the agreement not to disclose proprietary or confidential information.	No Exceptions Noted
	A clear desk policy for papers, removable storage media and a clear screen policy for information processing facilities is in place. Users are aware of their responsibility for ensuring unattended equipment is secure from unauthorized access.	Inspected the Secure Workspace Policy, the centralized workstation idle timeout configuration, and conducted a corroborative inquiry of management to determine that a clear desk policy for papers, removable storage media and a clear screen policy for information processing facilities was in place.	No Exceptions Noted
	Policies and procedures are in place to guide personnel on their responsibility for the classification of data and documents.	Inspected the Information Value Classification Policy and Procedures and conducted a corroborative inquiry of management to determine that policies were in place to guide personnel on their responsibility for the classification of documents and data related to the secure storage and destruction of sensitive data and documents.	No Exceptions Noted
	Policies and procedures are in place to guide personnel on their responsibility for the privacy and confidentiality of data and documents, and the allowed methods and purposes for disclosure.	Inspected the Electronic Content Policy and the Information Value Classification Policy and Procedures to determine that policies were in place to guide personnel on their responsibility for the privacy/confidentiality of documents and data and the allowed methods and purposes of such disclosure if any.	No Exceptions Noted

**Trust Services Principle – Confidentiality (Continued)**

*Information designated as confidential is protected as committed or agreed.*

C1.0	Additional criteria related to Confidentiality		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.		
	Management requires disk level encryption for laptops, portable devices and media.	Inspected the disk level encryption for the sampled laptops and conducted a corroborative inquiry of management to determine that management required disk level encryption for laptops, portable devices and media.	No Exceptions Noted
	Management controls the use of portable storage devices used for LNRS' business.	Inspected the centralized configuration preventing the use of portable storage devices and conducted a corroborative inquiry of management to determine that management prohibited the use of portable storage devices are controlled.	No Exceptions Noted
	Policies and procedures are in place to guide personnel on their responsibility for the retention of data and documents.	Inspected the Record Retention Schedule and conducted a corroborative inquiry of management to determine that policies were in place to guide personnel on their responsibility for the retention of documents and data related to the secure storage and destruction of sensitive data and documents.	No Exceptions Noted

## Trust Services Principle – Confidentiality (Continued)

Information designated as confidential is protected as committed or agreed.

C1.0	Additional criteria related to Confidentiality (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.		
	Documented procedures are in place to ensure all media are physically destroyed rendering all sensitive information unreadable before being discarded or recycled.	Inspected the Data Destruction Standards and an example certificate of destruction for physical media to determine that all a policy exists to guide personnel to destroy sensitive information before discarding assets.	No Exceptions Noted
	Policies and procedures are in place to guide personnel on their responsibility for the retention of data and documents.	Inspected the Record Retention Schedule and conducted a corroborative inquiry of management to determine that policies were in place to guide personnel on their responsibility for the retention of documents and data related to the secure storage and destruction of sensitive data and documents.	No Exceptions Noted
	Secured areas and shredding bins are utilized for the storage of sensitive documents and those awaiting destruction by a contracted third party shredding vendor.	Observed the secured shredding bins during onsite procedures and conducted a corroborative inquiry of management to determine that documents awaiting destruction were kept in secured locations.	No Exceptions Noted
	A third party vendor periodically retrieves and shreds sensitive documents contained in the secured containers.	Inspected the third party shredding invoices and conducted a corroborative inquiry of management to determine that the service was used.	No Exceptions Noted
	Documented procedures are in place to ensure all media are physically destroyed rendering all sensitive information unreadable before being discarded or recycled.	Inspected the Data Destruction Standards and an example certificate of destruction for physical media to determine that all a policy exists to guide personnel to destroy sensitive information before discarding assets.	No Exceptions Noted

## Trust Services Principle – Privacy

*Personal information is collected, used, retained, disclosed, and disposed to meet the entity's commitments and system requirements.*

P3.0	Privacy Criteria Related to Collection		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
P3.1	Personal information is collected consistent with the entity's objectives related to privacy.		
	The methods for collecting personal information and the adherence to applicable laws and regulations are reviewed by the legal department on an annual basis.	Inspected the Privacy Policy review date and conducted a corroborative inquiry of management to determine that the methods for collecting personal information and the adherence to applicable laws and regulations were reviewed by the legal department on an annual basis.	No Exceptions Noted
	LNRS requires all 3rd parties such as vendors and suppliers to sign contracts which provides guidance on security requirements and responsibilities.	Inspected the signed agreements for the sampled vendors and conducted a corroborative inquiry of management to determine that LNRS required all 3rd parties such as vendors and suppliers to acknowledge the information security policy which provided governance on connections to corporate resources.	No Exceptions Noted
	A Policy is in place to review and monitor the ongoing performance of the sub-service organizations.	Inspected the Third Parties Security Policy to determine that a Policy was in place to review and monitor the ongoing performance of the sub-service organizations.	No Exceptions Noted
	LNRS assesses the risks that vendors and business partners will fail to meet LNRS's requirements.	Inspected the third-party risk considerations to determine that LNRS assessed the risks that vendors and business partners will fail to meet LNRS's requirements.	No Exceptions Noted

## Trust Services Principle – Privacy (Continued)

*Personal information is collected, used, retained, disclosed, and disposed to meet the entity's commitments and system requirements.*

P4.0	Privacy Criteria Related to Use, Retention, and Disposal		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
P4.1	The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy.		
	The Privacy Policy is reviewed and updated when changes to the privacy practices of LNRS are implemented, those changes are made available to data subjects in a timely manner.	Inspected the Privacy Policy review date as available on LNRS' public web site and conducted a corroborative inquiry of management to determine that the Privacy Policy was reviewed and updated when changes to the privacy practices of LNRS were implemented, those changes were communicated to data subjects in a timely manner.	No Exceptions Noted
	Employees complete privacy awareness training on an annual basis to help ensure that employees understand their obligations and responsibilities to comply with the corporate and business privacy policies.	Inspected the privacy awareness training logs for the sampled active employees and conducted a corroborative inquiry of management to determine that employees completed privacy awareness training on an annual basis to help ensure that employees understood their obligations and responsibilities to comply with the corporate and business privacy policies.	No Exceptions Noted



## Trust Services Principle – Privacy (Continued)

*Personal information is collected, used, retained, disclosed, and disposed to meet the entity's commitments and system requirements.*

P4.0	Privacy Criteria Related to Use, Retention, and Disposal (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
P4.2	The entity retains personal information consistent with the entity's objectives related to privacy.		
	Administration rights to databases are restricted to only authorized personnel.	Inspected the authorized users for database access and conducted a corroborative inquiry of management to determine that access was restricted to only certain authorized administrators.	No Exceptions Noted
	Policies and procedures are in place to guide personnel on their responsibility for the retention of data and documents.	Inspected the Record Retention Schedule and conducted a corroborative inquiry of management to determine that policies were in place to guide personnel on their responsibility for the retention of documents and data related to the secure storage and destruction of sensitive data and documents.	No Exceptions Noted

## Trust Services Principle – Privacy (Continued)

*Personal information is collected, used, retained, disclosed, and disposed to meet the entity's commitments and system requirements.*

P4.0	Privacy Criteria Related to Use, Retention, and Disposal (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
P4.3	The entity securely disposes of personal information to meet the entity's objectives related to privacy.		
	Documented procedures are in place to ensure all media are physically destroyed rendering all sensitive information unreadable before being discarded or recycled.	Inspected the Data Destruction Standards and an example certificate of destruction for physical media to determine that all a policy exists to guide personnel to destroy sensitive information before discarding assets.	No Exceptions Noted
	Policies and procedures are in place to guide personnel on their responsibility for the handling of client information related to the secure storage and destruction of sensitive data and documents.	Inspected the Records Management Policy, the Information Value Classification Procedures, and conducted a corroborative inquiry of management to determine that policies were in place to guide personnel on their responsibility for the handling of client information related to the secure storage and destruction of sensitive data and documents.	No Exceptions Noted
	A third party vendor periodically retrieves and shreds sensitive documents contained in the secured containers.	Inspected the third party shredding invoices and conducted a corroborative inquiry of management to determine that the service was used.	No Exceptions Noted

## Trust Services Principle – Privacy (Continued)

*Personal information is collected, used, retained, disclosed, and disposed to meet the entity's commitments and system requirements.*

P5.0	Privacy Criteria Related to Access		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
P5.1	The entity grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy.		
	Documented procedures are in place to allow data subjects to update the personal data in the system.	Inspected the Privacy Policy as available on the public website and conducted a corroborative inquiry of management to determine that defined procedures were in place to allow data subjects to update their personal data in the system, if a denial of the request was issued the reasons for the denial was provided.	No Exceptions Noted
	Procedures are in place to respond to data subject inquiries related to personal data.	Inspected the data subject reporting process for disclosing personal data upon data subject request and conducted a corroborative inquiry of management to determine that procedures were in place to respond to data subject inquiries related to personal data.	No Exceptions Noted
	The privacy policy is available for individuals to view on LNRS' website to inform individuals how they may obtain access to their personal information to review, update, and correct that information.	Inspected the Privacy Policy as available on the public website and conducted a corroborative inquiry of management to determine that the privacy policy was available for individuals to view on LNRS' website to inform individuals how they may obtain access to their personal information to review, update, and correct that information.	No Exceptions Noted

## Trust Services Principle – Privacy (Continued)

*Personal information is collected, used, retained, disclosed, and disposed to meet the entity's commitments and system requirements.*

P5.0	Privacy Criteria Related to Access (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
P5.2	The entity corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy.		
	Documented procedures are in place to allow data subjects to update the personal data in the system.	Inspected the Privacy Policy as available on the public website and conducted a corroborative inquiry of management to determine that defined procedures were in place to allow data subjects to update their personal data in the system, if a denial of the request was issued the reasons for the denial was provided.	No Exceptions Noted
	Procedures are in place to ensure personal data is accurately maintained.	Inspected the Data Accuracy Policy for Consumer Reports and the supporting logical access controls to determine that procedures were in place to ensure personal data was accurately maintained.	No Exceptions Noted
	Procedures are in place to respond to data subject inquiries related to personal data.	Inspected the data subject reporting process for disclosing personal data upon data subject request and conducted a corroborative inquiry of management to determine that procedures were in place to respond to data subject inquiries related to personal data.	No Exceptions Noted

## Trust Services Principle – Privacy (Continued)

*Personal information is collected, used, retained, disclosed, and disposed to meet the entity's commitments and system requirements.*

P6.0	Privacy Criteria Related to Disclosure and Notification (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
P6.2	The entity creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to meet the entity's objectives related to privacy.		
	LNRS maintains an audit trail of all authorized disclosures of personal information.	Inspected the audit trail for an example authorized disclosure and conducted a corroborative inquiry of management to determine that audit trails of personal data disclosures were maintained.	No Exceptions Noted

## Trust Services Principle – Privacy (Continued)

*Personal information is collected, used, retained, disclosed, and disposed to meet the entity's commitments and system requirements.*

P6.0	Privacy Criteria Related to Disclosure and Notification (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
P6.3	The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity's objectives related to privacy.		
	LNRS has a Security Incident Response Policy and Procedures in place to provide policy guidance and establish responsibilities for responding to and reporting security breaches.	Inspected the Data Security Incident Response Overview and Incident Response and Notification Policy to determine that LNRS had a Security Incident Response Policy and Procedures in place to provide policy guidance for responding to and reporting security breaches.	No Exceptions Noted
	Policies and Procedures are in place for reporting breaches of personal data to affected data subjects and regulatory agencies.	Inspected the Incident Response and Notification Policy and conducted a corroborative inquiry of management to determine that Policies and Procedures were in place for reporting breaches of personal data to affected data subjects and regulatory agencies.	No Exceptions Noted

## Trust Services Principle – Privacy (Continued)

*Personal information is collected, used, retained, disclosed, and disposed to meet the entity's commitments and system requirements.*

P6.0	Privacy Criteria Related to Disclosure and Notification (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
P6.4	The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary.		
	A Policy is in place to review and monitor the ongoing performance of the sub-service organizations.	Inspected the Third Parties Security Policy to determine that a Policy was in place to review and monitor the ongoing performance of the sub-service organizations.	No Exceptions Noted
	LNRS requires all 3rd parties such as vendors and suppliers to sign contracts which provides guidance on security requirements and responsibilities.	Inspected the signed agreements for the sampled vendors and conducted a corroborative inquiry of management to determine that LNRS required all 3rd parties such as vendors and suppliers to acknowledge the information security policy which provided governance on connections to corporate resources.	No Exceptions Noted
	LNRS maintains procedures to ensure 3rd party vendors comply with the Privacy Policy.	Inspected the privacy clauses in the Service Contractor Agreement and conducted a corroborative inquiry of management to determine that LNRS maintained procedures to ensure 3rd party vendors complied with the Privacy Policy.	No Exceptions Noted

## Trust Services Principle – Privacy (Continued)

*Personal information is collected, used, retained, disclosed, and disposed to meet the entity's commitments and system requirements.*

P6.0	Privacy Criteria Related to Disclosure and Notification (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
P6.5	The entity obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's objectives related to privacy.		
	LNRS requires all 3rd parties such as vendors and suppliers to sign contracts which provides guidance on security requirements and responsibilities.	Inspected the signed agreements for the sampled vendors and conducted a corroborative inquiry of management to determine that LNRS required all 3rd parties such as vendors and suppliers to acknowledge the information security policy which provided governance on connections to corporate resources.	No Exceptions Noted
	LNRS maintains procedures to ensure 3rd party vendors comply with the Privacy Policy.	Inspected the privacy clauses in the Service Contractor Agreement and conducted a corroborative inquiry of management to determine that LNRS maintained procedures to ensure 3rd party vendors complied with the Privacy Policy.	No Exceptions Noted
	LNRS has a Security Incident Response Policy and Procedures in place to provide policy guidance and establish responsibilities for responding to and reporting security breaches.	Inspected the Data Security Incident Response Overview and Incident Response and Notification Policy to determine that LNRS had a Security Incident Response Policy and Procedures in place to provide policy guidance for responding to and reporting security breaches.	No Exceptions Noted



## Trust Services Principle – Privacy (Continued)

*Personal information is collected, used, retained, disclosed, and disposed to meet the entity's commitments and system requirements.*

P6.0	Privacy Criteria Related to Disclosure and Notification (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
P6.6	The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.		
	Documented procedures are in place for communicating to or from Law Enforcement Agencies.	Inspected the Incident Response and Notification Policy to determine that documented procedures are in place for communicating to or from Law Enforcement Agencies.	No Exceptions Noted
	Policies and Procedures are in place for reporting breaches of personal data to affected data subjects and regulatory agencies.	Inspected the Incident Response and Notification Policy and conducted a corroborative inquiry of management to determine that Policies and Procedures were in place for reporting breaches of personal data to affected data subjects and regulatory agencies.	No Exceptions Noted

**Trust Services Principle – Privacy (Continued)**

*Personal information is collected, used, retained, disclosed, and disposed to meet the entity's commitments and system requirements.*

P6.0	Privacy Criteria Related to Disclosure and Notification (Continued)		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
P6.7	The entity provides data subjects with an accounting of the personal information held and disclosure of the data subjects' personal information, upon the data subjects' request, to meet the entity's objectives related to privacy.		
	LNRS maintains an audit trail of all authorized disclosures of personal information.	Inspected the audit trail for an example authorized disclosure and conducted a corroborative inquiry of management to determine that audit trails of personal data disclosures were maintained.	No Exceptions Noted
	Procedures are in place for reporting to data subjects upon request of personal data records and disclosures.	Inspected the data subject reporting process for disclosing personal data upon data subject request and conducted a corroborative inquiry of management to determine that procedures were in place for reporting to data subjects upon request of personal data records and disclosures.	No Exceptions Noted
	Procedures are in place to respond to data subject inquiries related to personal data.	Inspected the data subject reporting process for disclosing personal data upon data subject request and conducted a corroborative inquiry of management to determine that procedures were in place to respond to data subject inquiries related to personal data.	No Exceptions Noted
	A customer support address and links to privacy-related request forms are provided within the privacy policy to allow individuals to determine whether LNRS maintains personal information about them and request access to their personal information.	Inspected the contact information and the privacy-related request forms as available on LNRS' public website to determine that a customer support e-mail address was provided within the privacy policy to allow individuals to determine whether LNRS maintained personal information about them and request access to their personal information.	No Exceptions Noted

## Trust Services Principle – Privacy (Continued)

*Personal information is collected, used, retained, disclosed, and disposed to meet the entity's commitments and system requirements.*

P7.0	Privacy Criteria Related to Quality		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
P7.1	The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy.		
	Documented procedures are in place to allow data subjects to update the personal data in the system.	Inspected the Privacy Policy as available on the public website and conducted a corroborative inquiry of management to determine that defined procedures were in place to allow data subjects to update their personal data in the system, if a denial of the request was issued the reasons for the denial was provided.	No Exceptions Noted
	Procedures are in place to ensure personal data is accurately maintained.	Inspected the Data Accuracy Policy for Consumer Reports and the supporting logical access controls to determine that procedures were in place to ensure personal data was accurately maintained.	No Exceptions Noted
	Procedures are in place to respond to data subject inquiries related to personal data.	Inspected the data subject reporting process for disclosing personal data upon data subject request and conducted a corroborative inquiry of management to determine that procedures were in place to respond to data subject inquiries related to personal data.	No Exceptions Noted
	A customer support address and links to privacy-related request forms are provided within the privacy policy to allow individuals to determine whether LNRS maintains personal information about them and request access to their personal information.	Inspected the contact information and the privacy-related request forms as available on LNRS' public website to determine that a customer support e-mail address was provided within the privacy policy to allow individuals to determine whether LNRS maintained personal information about them and request access to their personal information.	No Exceptions Noted

**Trust Services Principle – Privacy (Continued)**

*Personal information is collected, used, retained, disclosed, and disposed to meet the entity's commitments and system requirements.*

P8.0	Privacy Criteria Related to Monitoring and Enforcement		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
P8.1	The entity implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken in a timely manner.		
	Procedures are in place for reporting to data subjects upon request of personal data records and disclosures.	Inspected the data subject reporting process for disclosing personal data upon data subject request and conducted a corroborative inquiry of management to determine that procedures were in place for reporting to data subjects upon request of personal data records and disclosures.	No Exceptions Noted
	Procedures are in place to ensure personal data is accurately maintained.	Inspected the Data Accuracy Policy for Consumer Reports and the supporting logical access controls to determine that procedures were in place to ensure personal data was accurately maintained.	No Exceptions Noted
	Procedures are in place to respond to data subject inquiries related to personal data.	Inspected the data subject reporting process for disclosing personal data upon data subject request and conducted a corroborative inquiry of management to determine that procedures were in place to respond to data subject inquiries related to personal data.	No Exceptions Noted
	A customer support address and links to privacy-related request forms are provided within the privacy policy to allow individuals to determine whether LNRS maintains personal information about them and request access to their personal information.	Inspected the contact information and the privacy-related request forms as available on LNRS' public website to determine that a customer support e-mail address was provided within the privacy policy to allow individuals to determine whether LNRS maintained personal information about them and request access to their personal information.	No Exceptions Noted

**Trust Services Principle – Privacy (Continued)**

*Personal information is collected, used, retained, disclosed, and disposed to meet the entity's commitments and system requirements.*

P8.0	Privacy Criteria Related to Monitoring and Enforcement		
TSP	Description of Controls in Place	Service Auditor's Test of Controls	Test Results
P8.1	The entity implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken in a timely manner.		
	The privacy policy addresses the monitoring and enforcement of privacy policies and procedures.	Inspected the Privacy Policy as available on the public website and conducted a corroborative inquiry of management to determine that the privacy policy addressed the monitoring and enforcement of privacy policies and procedures.	No Exceptions Noted
	The privacy policy is available for individuals to view on LNRS' website to inform individuals how they may obtain access to their personal information to review, update, and correct that information.	Inspected the Privacy Policy as available on the public website and conducted a corroborative inquiry of management to determine that the privacy policy was available for individuals to view on LNRS' website to inform individuals how they may obtain access to their personal information to review, update, and correct that information.	No Exceptions Noted

## SECTION V – OTHER INFORMATION PROVIDED BY LEXISNEXIS RISK SOLUTIONS

## Management's Responses to Noted Exceptions

Description of Controls in Place	Service Auditor's Test of Controls
LNRS conducts periodic vendor assessments (based on vendor classification) to evaluate assessment results and review any independent 3 <sup>rd</sup> party assessments on contracted subservice organizations and vendors.	Inspected the vendor review assessments for the sample selected vendors to determine that LNRS has documented procedures for onboarding new vendors.
One (1) of the eighteen (18) sampled vendors did not have a review conducted in a timely manner.	
<p><i>Management's Response: In an effort to account for the complexity and overall engagement process of vendor assessments, we increased the frequency of reporting used to identify vendor assessments expiring within the next 60 days to a weekly cadence. This will give us the ability to initiate the assessment renewal process in a more timely manner by immediate contact with the vendor and business owner to achieve completion by the desired expiration date.</i></p>	