UHY LLP
Certified Public Accountants

LATITUDE
SUBROGATION SERVICES

Inspection Connection

Latitude Subrogation Services, LLC and InspectionConnection, LLC

Subrogation and Salvage Recovery System and Vehicle Material Damage Appraisal System

SOC 2® Type 2

April 1, 2022 – March 31, 2023

UHY LLP
www.uhy-us.com

The next level of service

TABLE OF CONTENTS

Section 1:

Independent Service Auditor's Report

INDEPENDENT SERVICE AUDITOR'S REPORT

To the Board of Latitude:

Scope

We have examined Latitude Subrogation Services, LLC's ("LSS") accompanying description of its subrogation and salvage recovery services system and InspectionConnection, LLC's ("IC") accompanying description of its vehicle material damage appraisal services system (collectively referred to as "Latitude system") found in Section 3 titled "Latitude's Description of Its Subrogation and Salvage Recovery Services and Vehicle Material Damage Appraisal Services System" throughout the period April 1, 2022 to March 31, 2023 ("description") based on the criteria for a description of a service organization's system set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022)* in AICPA, *Description Criteria*, ("description criteria") and the suitability of the design and operating effectiveness of controls stated in the description throughout the period April 1, 2022 to March 31, 2023, to provide reasonable assurance that Latitude's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability ("applicable trust services criteria") set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* in AICPA, *Trust Services Criteria*.

The information included in Section 5, "Other Information Provided by Latitude That Is Not Covered by the Service Auditor's Report," is presented by Latitude's management to provide additional information and is not a part of Latitude's description of its subrogation and salvage recovery services and vehicle material damage appraisal services system made available to user entities during the period April 1, 2022 to March 31, 2023. Information about Latitude management's responses to exceptions has not been subjected to the procedures applied in the examination and accordingly, we express no opinion on it.

Latitude uses subservice organizations to provide Software as a Service (SaaS) and Infrastructure as a Service (IaaS) solutions services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Latitude, to achieve Latitude's service commitments and system requirements based on the applicable trust services criteria. The description presents Latitude's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Latitude's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

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

Service Organization's Responsibilities

Latitude 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 Latitude's service commitments and system requirements were achieved. In Section 2, Latitude has provided the accompanying assertion titled Latitude Management's Assertion ("assertion") about the description and the suitability of design and operating effectiveness of controls stated therein. Latitude is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

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

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

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 those tests are listed in Section 4, "Trust Services Criteria, Related Controls, and Tests of Controls" of this report.

Opinion

In our opinion, in all material respects—

a. the description presents Latitude's subrogation and salvage recovery services and vehicle material damage appraisal services system that was designed and implemented throughout the period April 1, 2022 to March 31, 2023 in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period April 1, 2022 to March 31, 2023 to provide reasonable assurance that Latitude's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of Latitude 's controls throughout that period.

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

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of Latitude; user entities of Latitude's subrogation and salvage recovery services and vehicle material damage appraisal services system during some or all of the period April 1, 2022 to March 31, 2023, business partners of Latitude subject to risks arising from interactions with the subrogation and salvage recovery services and vehicle material damage appraisal services system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties.
- Internal control and its limitations.
- Complementary user entity controls and complementary subservice organization 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.

Farmington Hills, Michigan
August 28, 2023

Section 2:

Latitude Management's Assertion

Management of Latitude's Assertion:

We have prepared the accompanying description of Latitude Subrogation Services, LLC's ("LSS") subrogation and salvage recovery services system and InspectionConnection, LLC's ("IC") vehicle material damage appraisal services system (collectively referred to as "Latitude system") titled "Latitude's Description of Its Subrogation and Salvage Recovery Services and Vehicle Material Damage Appraisal Services System" throughout the period April 1, 2022 to March 31, 2023 ("description") based on the criteria for a description of a service organization's system set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022)* in AICPA, *Description Criteria* ("description criteria"). The description is intended to provide report users with information about the subrogation and salvage recovery services and vehicle material damage appraisal services systems that may be useful when assessing the risks arising from interactions with Latitude's system, particularly information about system controls that Latitude has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability ("applicable trust services criteria") set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* in AICPA, *Trust Services Criteria*.

Latitude uses subservice organizations to provide Software as a Service (SaaS) and Infrastructure as a Service (IaaS) solutions. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Latitude, to achieve Latitude's service commitments and system requirements based on the applicable trust services criteria. The description presents Latitude's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Latitude's controls. The description does not disclose the actual controls at the subservice organizations.

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

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

1) The description presents Latitude's subrogation and salvage recovery services and vehicle material damage appraisal services system that was designed and implemented throughout the period April 1, 2022 to March 31, 2023 in accordance with the description criteria.
2) The controls stated in the description were suitably designed throughout the period April 1, 2022 to March 31, 2023 to provide reasonable assurance that Latitude's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of Latitude's controls throughout that period.
3) The controls stated in the description operated effectively throughout the period April 1, 2022 to March 31, 2023 to provide reasonable assurance that Latitude's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Latitude's controls operated effectively throughout that period.

Marc Hassen
Chief Operating Officer

Section 3:

Latitude's Description of its Subrogation and Salvage Recovery Services and Vehicle Material Damage Appraisal Services System

OVERVIEW

Latitude Subrogation Services, LLC ("LSS") is a privately held company established in 2000 to provide subrogation and salvage recovery services to insurers, self-insured entities, third party administrators, specialty risk companies, and other clients as a vendor and purchaser of subrogation assets, specializing in Auto, Property, and Workers Compensation. The company is headquartered in Bloomfield Hills, Michigan, and provides services in the United States and Canada.

The company acquired the International Insurance Institute, Inc. ("III") in 2020, which provides claim training services, and InspectionConnection, LLC ("IC") in 2021, which provides material damage claim handling services such as vehicle repair appraisals and related services.

SCOPE OF THE SYSTEM

The scope of this report includes the subrogation and salvage recovery services provided in the United States and Canada by LSS as well as the vehicle material damage estimating-related services provided by IC (collectively referred to as "Latitude" or "Company") for the period April 1, 2022 through March 31, 2023. The scope of this attestation does not include services provided by III.

Subservice Organizations

Latitude utilizes third-party providers ("subservice organizations") to host the Company's subrogation and salvage recovery services and vehicle material damage appraisal services system. The subservice organizations and the services provided include:

Subservice Organization	Services Provided
Salesforce Service Cloud	Software as a Service (SaaS) solution used to host the LSS Claims Management System and SubroChain®.
Microsoft Corporation	Microsoft 365 (M365) SaaS solution used within SubroChain® for client subrogation claim activity communications and reporting as well as the client claim referral process. M365 SharePoint is used to track Salvage claim quoting activities performed by IC.
Microsoft Azure Cloud	Infrastructure as a Service (IaaS) platform used to host the LSS Client Access Portal and associated data warehouse.

The scope of this report includes only Latitude's subrogation and salvage recovery services and vehicle material damage appraisal services system and does not include the controls in place at the subservice organizations.

Not Applicable Trust Services Criteria

There are no Trust Services criteria that are not applicable to Latitude's subrogation and salvage recovery services and vehicle material damage appraisal services system.

Significant Changes to the System

There were no significant changes to the in-scope services system during the attestation period. Any changes to the service organization's control activities or processes related to the in-scope services system are included in Section 4, "Information Provided by the Independent Service Auditor."

Significant Subsequent Events

There were no significant events subsequent to the attestation period and through the date of the report that would materially impact the in-scope services system.

Significant Events

The COVID-19 pandemic had minimal impact on Latitude as the Company has for many years utilized a remote staffing model. Most employees work from their homes.

Identified System Incidents

No significant incidents have occurred related to the services provided to user entities during the review period.

DESCRIPTION OF THE SERVICE OFFERINGS PROVIDED

Subrogation

Clients assign subrogation claims to LSS to obtain financial recoveries they have paid to one party, that are the legal responsibility of another party ("responsible party"). The specific subrogation claim lifecycle transactions and processes vary depending on the agreement with the client.

Assignments

Clients assign subrogation claims to LSS for handling in one of the following ways. LSS will provide the client with an acknowledgement of the assignment depending on the client agreement.

First Notice of Loss (FNOL)	The client provides LSS with a data file upon their receipt of a first notice of loss on a claim. Latitude may open a subrogation claim based on a review of the FNOL information.
Referral	The client refers a claim to LSS for subrogation, typically via email though other channels are possible.
Closed File Review (CFR)	LSS reviews closed files and identify claims that still have subrogation potential.

Subrogation

A Subrogation Specialist is assigned the claim. The Specialist investigates the claim, identifies responsible parties, issues recovery demands, negotiates or arranges for recovery payments, and provides claim notes throughout the process.

The client's claim notes, documents, and payment history are needed by LSS to handle the claim. This information may be provided by a client adjuster, or the client may provide LSS employees, such as the Claims Support team, with access to their system so that LSS can retrieve the information directly. A variety of data exchange mechanisms are supported.

Claims may also be litigated, arbitrated, or sent to a collection agency business partner if appropriate. Special handling "workflow" will be followed where required by a client, such as client approval for litigation.

Recoveries

Responsible parties (such as adverse insurance companies) make payments directly to LSS or to the client. Payments made to LSS may be received via check or electronically and are processed by LSS's accounting team.

Remittance To Client

LSS provides clients with recovery payment remittance in accordance with the client agreement. Typically, remittance is provided monthly and is net of LSS's fee based on a contingency rate. Clients may instead choose to receive payment in full and be invoiced separately for LSS's fee. Remittance may be via check or ACH. A report listing the claims and payments is provided to the client with their remittance.

Reporting

LSS provides a proprietary reporting portal called Client Access Portal (LCAP) to clients. This site provides clients with the ability to see detailed information for all their subrogation claims they assigned to LSS. Claim data is automatically synced to LCAP from LSS's core processing system, SubroChain®. LSS may also provide the client with customized or ad hoc reporting on demand.

A summary of recovery payments is provided for each claim when the claim is closed If required by the client.

Salvage

Clients engage LSS to assist obtaining financial salvage proceeds on total loss vehicles, typically by helping coordinate the sale of the vehicle through a "salvor" (e.g., vehicle auction facility or "pool"). Variations apply such as when an owner wishes to retain a totaled vehicle or the vehicle is stolen.

Assignment

The client refers a salvage claim to LSS via email.

Gather Title Work

The Salvage Specialist contacts the vehicle owner and obtains the necessary paperwork to facilitate the transfer of the title from the previous owner to the client, or purchaser of the vehicle.

Lien Resolution

The Salvage Specialist contacts a lienholder (such as a bank) if a loan is outstanding to identify the payoff amount and obtain a release.

Vehicle Sale

The paperwork is provided to the salvor auction facility and the claim is monitored for sale of the vehicle and handling of any salvor charges.

Remittance

Sale proceeds may be sent directly from the salvor to the client, or from the salvor to LSS. In the latter case, LSS will accumulate and remit proceeds to the client.

Fee

The client is invoiced for the agreed flat fee following the closure of the assignment.

Material Damage Claim Handling (InspectionConnection)

Clients assign material damage claims to IC to create estimates, review existing estimates, review in-bound subrogation demands, and/or establish the value of personal automobiles and commercial, and mobile units.

Assignments

Clients will assign claims in their preferred method.

1. Claims are assigned via the www.ic-claims.com website
2. Claims are assigned via a custom link for their company via the GN360 Global Net program

3. Claims are assigned via email to claims@ic-claims.com website
4. Claims are assigned via the CCC portal

Claim Handling

Once an assignment is received by IC, it is assigned to the appropriate Appraiser for completion. These claims are distributed based on the skill sets of the IC Appraiser or the needs of the client. IC Appraisers will complete one of the following:

- Create a damage appraisal
- Review an existing estimate for appropriateness
- Evaluate, review, and advise appropriate indemnity-spend on in-bound subrogation demands
- Establish the "actual cash value" of a unit via industry accepted standards

Quality Assurance

Each month, all IC claim associates have a random sample of worked claims thoroughly reviewed by leadership. This process investigates each portion of the IC work product for accuracy and adherence to any client specific needs.

Compensation

Clients are billed at the end of each month based on their specific needs. These are sent from the Latitude Accounting department where all aspects of the invoicing and proceeds processing occur.

Reporting

Clients are provided a report of files reviewed each quarter. They are also provided with measurements on claim volume, cycle time and any indemnity impact IC was able to provide. These reports are generated in the SharePoint environment.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Latitude's Platform is designed to automate manual insurance subrogation, salvage, and material damage estimating processes and procedures to meet its objectives for providing those services. Those objectives are based on the service commitments that Latitude makes to clients, the laws and regulations that govern the services, and the financial, operational, and compliance requirements that Latitude has established for their services. The services of Latitude are subject to the security and privacy requirements of state privacy laws and regulations in the jurisdictions in which Latitude operates.

Security commitments are industry standards and include, but are not limited to, the following:

- Role Based Access Control for all users and clients for applicable systems that permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role
- Use of encryption technologies to protect customer data both at rest and in transit
- Use of Multifactor authentication to critical systems
- Timely Onboarding and Offboarding user procedures to allow and restrict unauthorized access

Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the Latitude Platform is designed, modified, operated, and managed. In addition to these policies, standard operating procedures have been documented on how to execute manual and automated processes required for support of the Latitude Platform.

Availability commitments

Latitude provides the Client Access application (see below) to enable clients to view information related to the subrogation and salvage claims they have assigned to LSS.

COMPONENTS OF THE SYSTEM

System Boundaries

The elements of our system include the infrastructure, software, people, procedures, and data responsible for supporting the Latitude Platform.

Infrastructure

The Latitude Platform consists of multiple cloud hosted SaaS and IaaS solutions and providers that have evolved to provide and track an array of services for our clients. The main component of the Subrogation Platform is called SubroChain® (see diagram below) which is a SaaS solution that runs on the Salesforce Service Cloud. The SubroChain® environment has a unique Salesforce instance number that designates the specific software, server, and network infrastructure used which are maintained by Salesforce staff and contracted services. LSS is responsible for making changes to the user interface and database entries of SubroChain®, along with change management, backup and restoration of those changes.

The Client Access system is an IaaS solution implemented on Azure cloud and is comprised of Microsoft SQL and web servers. Microsoft staff and contractors maintain all server and network hardware as well as operating systems and software code. LSS is responsible for operating system (OS) patching, user interface code configurations and database maintenance.

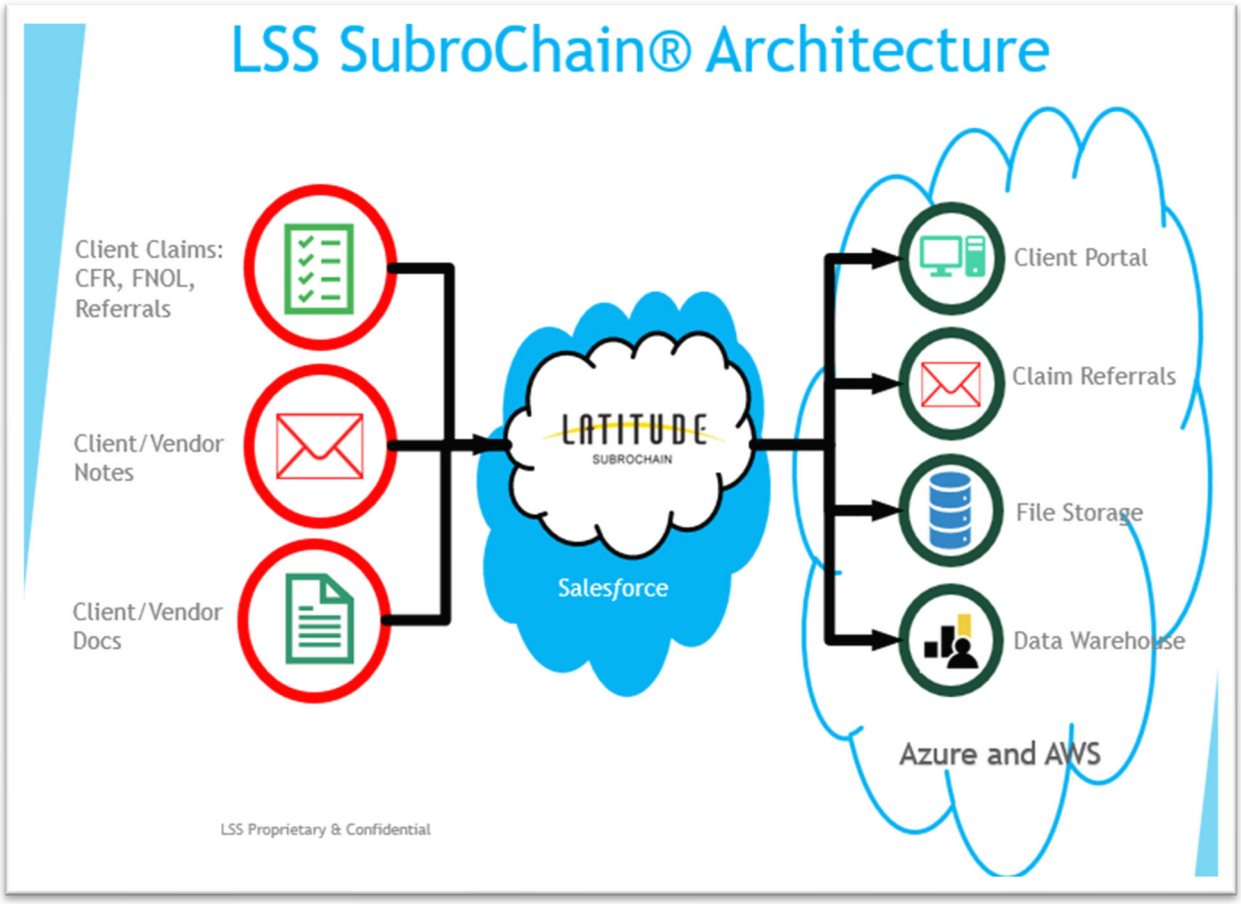
Latitude uses Microsoft's 365 (M365) SaaS solution to send status updates and receive work requests from our clients via email. M365 runs on the Microsoft Azure Cloud. Latitude has a unique Tenant ID number that designates the specific software, server, and network infrastructure used for M365 which are maintained by Microsoft's staff and contracted services. Latitude is responsible for administering user access, restricting or enforcing email addresses, limiting mailbox sizes, as well as backup and restoration of individual user accounts.

Latitude has designed and built a custom SharePoint list called ICT. This SaaS solution uses M365 SharePoint to enter, store, report, and export data that involves work activities received from IC clients. M365 SharePoint runs on the Microsoft Azure Cloud. LSS has a unique Tenant ID number that designates the specific software, server, and network infrastructure used for SharePoint which are maintained by Microsoft's staff and contracted services. Latitude is responsible for administering user access, creating reports, exporting data, and changing the User Interface layout for the SharePoint list. Latitude is also responsible for backing up and restoration of the SharePoint environment.

Remote LSS employees access the SubroChain® application through their company-supplied, protected, and secured computers. Some LSS users reside in our corporate office and utilize company computers, network, firewall, and Internet services provided and maintained by LSS IT staff and contracted services. LSS customers access LCAP using SSL through a web browser on their personally owned and operated computer.

Data communications between both SubroChain® and Client Access are encrypted using Transport Layer Security (TLS) as part of the HTTPS encryption protocol.

SubroChain® utilizes the Salesforce database to store client and claim subrogation information, which is encrypted using the Salesforce database encryption method to protect data at rest. The database, application and web servers are housed in Salesforce's secured data centers. LCAP uses the SQL database and associated 256-bit AES encryption methods to protect data at rest. The LCAP database and web servers are hosted in the Azure cloud and secured by Microsoft.



Software

The SubroChain® claim management system is a multiuser, Salesforce SaaS cloud application that is used to manage the activities and flow of information between LSS and their subrogation and salvage clients. This claims solution allows LSS users to enter, modify and retrieve information about the subrogation and salvage claims they are assigned. It also provides performance reports to help LSS users manage their workload. To access the site, LSS users must pass two-factor challenges from a mandatory authenticator mobile app provided and maintained by Salesforce.

A data warehouse is synced to SubroChain® and resides on a Microsoft SQL database. This SQL server is hosted in Azure and backed up using a Microsoft or Veeam backup solution. The data warehouse is used to provide reporting outside of the SubroChain® system including LCAP.

LCAP is a Microsoft Windows web-based application developed and maintained by Latitude contracted and internal IT staff. LCAP is hosted on a Windows server in Azure. LSS enhances and maintains LCAP to provide a self-service web portal for the company's subrogation clients to obtain information about their claims. The LCAP system displays SubroChain® data via the data warehouse hosted in Azure. LCAP is accessible for reviewing daily activities (notes), generating reports, and for historical claim progress monitoring. The information can be retrieved, reviewed, and reported as needed to create a history of approvals and denials for any claim submitted to LSS. Information can be retrieved by claim number, date, and type. To access the site, clients must request access for their unique company role.

The InspectionConnection Claims Tracker (ICT) solution is like the SubroChain® claim management solution, except its focus is on a small subset of material damage estimating quoting work. Material damage estimating claims are placed in a SharePoint list within the M365 suite of SaaS applications. After a user has successfully logged in, he or she is able to enter or modify new or existing claims, view pending and processed work, close pending claims, and create reports on existing claims.

Microsoft and Veeam backup solutions are used by Latitude staff and contracted services to create daily and weekly backups of the M365, LCAP data warehouse, and ICT SharePoint environments. The Latitude data warehouse resides on a Microsoft SQL server and is operated as an IaaS solution in Azure's cloud. The data warehouse is synced hourly with data fields from SubroChain® for reporting, backup, and data restoration purposes.

People

Latitude has a staff of approximately 110 employees organized in the following functional areas .

- Business Development – This group is responsible for all new business development for the company as well as account management, including arrangements for any special client requirements (aka "workflow").
- Claims – Subrogation and Salvage Specialists are assigned client claims and handle them through to completion.
- Claims Support – This team completes tasks to support Claims, such as obtaining notes, documents, and payment history from client systems and, where required, copying, and pasting LSS claim notes into client systems.
- Quality – The Quality team completes claim audits of Subrogation and Salvage Specialists activities on a sample basis.
- Accounting – The Accounting staff supports the company in all traditional Finance and Accounting functions such as General Ledger, Accounts Payable, Accounts Receivable, etc. including posting responsible party recovery payments into the SubroChain® system and preparing and providing remittance to clients.
- Human Resources – Manages the recruitment and retention of employees, as well as benefit programs, background checks and employee engagement.
- IT – Help desk, IT infrastructure, IT networking, IT system administration, software systems development and application support, information security, reporting, and IT operations personnel manage electronic interfaces and business implementation support and telecom.
    - The help desk group provides technical assistance to SubroChain®, LCAP and ICT users.
    - The infrastructure, networking, and systems administration staff typically have no direct use of the LSS or IC systems. Rather, it supports LSS's IT infrastructure, which is used by the software. A systems administrator will deploy the software and code change releases for SubroChain® and other systems into the production environment.
    - The software development staff develops and maintains the custom software for LSS. This includes the LCAP and ICT systems and their supporting cloud services. The staff includes software developers, database administration, and technical writers.
    - The information security staff supports SubroChain®, LCAP and ICT indirectly by monitoring internal and external security threats and maintaining current antivirus and anti-Malware software.
    - The information security staff maintains the inventory of IT assets.
    - IT operations manage the user access, backups, and reporting for the LCAP. This includes processing user membership and data files, producing reports, and resolving user issues.
    - Telecom personnel maintain the voice communications environment, provide user support to LSS, and resolve communication problems. This group does not directly use LSS systems, but it provides infrastructure support as well as disaster recovery assistance.

Processes and Procedures

Management has developed and communicated to LSS IT employees the procedures to restrict logical access to SubroChain®. Changes to these procedures are performed annually and authorized by senior management. These procedures cover the following key security life cycle areas:

- Data classification (data at rest, in motion, and output)
- Categorization of information
- Assessment of the business impact resulting from proposed security approaches
- Selection, documentation, and implementation of security controls
- Performance of annual management self-assessments to access security controls
- Authorization, changes to, and termination of information system access
- Monitoring security controls
- Management of access and roles
- Maintenance and support of the security system and necessary backup and offline storage
- Incident response
- Maintenance of restricted access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls)

Data

Data, as defined by LSS, constitutes the following:

Data Classification	Definition
User Role/Access Data	Data used to manage access to administrative roles or sensitive system functions.
Client Content	Client content including PII, reports, and insurance claim information.
Personal Identifiable Information (PII)	Data unique to a person or generated from a user's use of an LSS service: - Linkable to an individual user, contractor, or employee - Does not contain Client Content
Error logs	System data that does not contain Client Content, PII, or Account Data.
System Metadata	Data generated while running the service, which is not linkable to an individual user and does not contain Client Content, PII, or Account Data.
Account Data	Client contact, address, and role Data

Data for claims is received by various methods including SFTP and email from LSS clients and is automatically or manually entered in SubroChain®. LSS users edit the date fields in SubroChain®. Subrogation processing is initiated by the receipt of a new claim (FNOL) or existing claim (referral). This request typically comes directly from a client email or SFTP process. Reporting on the data sets is done in SubroChain® and on LCAP.

Client reports are available in LCAP and can be exported electronically but are limited based on job function. Reports can also be delivered externally using a Latitude purchased SaaS solution called Rubex. Latitude assigns Rubex accounts to clients and vendors when requested and the solution uses Transport Layer Security to encrypt all file exchanges.

RELEVANT ASPECTS OF INTERNAL CONTROLS

The security and availability categories and applicable trust services criteria were used to evaluate the suitability of design and operating effectiveness of controls stated in the description. Security criteria and the controls designed, implemented, and operated to meet them ensure that the system is protected against unauthorized access (both physical and logical), unauthorized disclosure of information, and damage to systems that could affect the entity's ability to meet its objectives. Availability criteria and supporting controls ensure the Company's information and systems are available for operation and use to meet its objectives.

The controls supporting the applicable trust services security and availability criteria are included in Section 4 of this report. Although the applicable trust services criteria and related controls are included in Section 4, they are an integral part of Latitude's description of the Latitude Platform.

Control Environment

Latitude's control environment, established and maintained by leadership, sets the tone for the organization and influences how employees perform their activities and carry out their control responsibilities. It also provides reasonable assurance to our clients and business partners that we are able to meet our service commitments and system requirements. The components of our control environment include our core values, management oversight, organizational structure, and our commitment to competence and accountability.

Integrity and Ethical Values

Latitude's core values including honesty, fairness and integrity are reflected in expectations, such as the handling of confidential information, set for employee conduct in the Employee Handbook and accompanying Acknowledgement. Background checks are completed for new hire candidates, and new employees acknowledge the handbook upon hire and whenever there is a change. Performance evaluations are completed during the new hire probationary period and annually thereafter, and a disciplinary action policy is in place to deal with violations of company policy, misconduct, and inadequate performance.

Risk Assessment

A strategic level risk assessment is completed by the executive team annually to identify, prioritize, and track mitigation on the most important risks to the company, such as fraud or market risk. A risk owner is identified to assess and pursue improvements where needed. Risks inherent to the subrogation and salvage process have been identified, and best practice guidelines defined to prevent those risks from occurring. Supervisor spot checks and quality team audits are used to help identify any problems so that corrective action and coaching can be implemented.

The Enterprise Risk Management process incorporates changes into its periodic reassessment of risk.

As a financial recovery service provider whose primary purpose is to recovery money from responsible parties on behalf of its clients, Latitude considers payment fraud to be the primary risk to the achievement of responsible stewardship of recoveries. Management maintains a risk and control assessment for payment fraud and periodically assesses controls for improvements.

Risk Mitigation

Latitude performs an annual risk assessment that covers security, continuity, and operational risks. As part of this process, threats to security are identified and the risk from these threats is formally assessed. The information gained from the assessment is used to create and prioritize work items.

Control Activities

Data communications between both SubroChain® and Client Access are encrypted using Transport Layer Security (TLS) as part of the HTTPS encryption protocol.

SubroChain® uses the Salesforce database and is encrypted using the Salesforce database encryption method to protect data at rest. The database, application, and web servers are housed in Salesforce's secured network operations centers (NOCs). LCAP uses the SQL database and associate encryption methods to protect data at rest. The LCAP database and web servers are hosted in the Azure cloud and secured by Microsoft.

Access Provisioning and Review (Logical and Physical)

When individuals join the company, HR creates an onboarding IT HD ticket for the new employee. Access for new employees is added based on role or special instruction in the IT ticket to respective service production environments. The ticket is closed when all accounts are created and company equipment is sent to and configured by Latitude IT staff.

When individuals leave the company, HR creates an offboarding IT HD ticket for the terminated employee. Access for terminated employees is then removed from respective service production environments and Latitude office door access. The ticket is closed when all accounts and access is removed, and company equipment is returned to Latitude.

A manual user access review is performed on a periodic basis to substantiate that access for each user, including third parties, is relevant and in line with job responsibilities. Any needed access alterations identified during the review are addressed in a timely manner.

Physical Security

Latitude operates door biometric access systems, alarm system and security camera system. New employees are added to the appropriate doors upon hire or as requested by management. Door and alarm access is removed upon termination.

Network Security

Latitude uses Azure AD infrastructure with MFA for centralized authentication and authorization to their endpoints and M365 service. Salesforce database and authenticator app are used to control access to SubroChain® and SQL database is used to control access to LCAP.

Each Latitude endpoint including computers and servers has an antimalware agent installed. The antimalware agent is configured to obtain the latest available definition files from the antimalware server hosted on the Internet. If there are issues related to the agent synchronization process with the antimalware server, the individual antimalware agent automatically notifies the IT team, and the reported issue is analyzed and resolved.

Data Transmission Security

LSS encrypts the hard drive of all company supplied user computers, deactivates USB ports to prevent removal of information, and removes administrative control to the computer operating systems for all LSS and IC staff.

Data communications between both Clients and the LCAP system are encrypted using Transport Layer Security (TLS) as part of the HTTPS encryption protocol. LSS provides a SFTP server to securely transfer client data from client systems to SubroChain®. Revver is also used to transfer client data to and from clients utilizing TLS, passwords, and user IDs to secure the transmission and access.

The SubroChain® uses the Salesforce database and is encrypted using the Salesforce database encryption service to protect data at rest. The database, application, and web servers are housed in Salesforce's secured network operations centers (NOCs). LCAP uses the SQL database and associate encryption methods to protect data at rest. The LCAP database and web servers are hosted in the Azure cloud and secured by Microsoft.

Data, Software, and Hardware Disposal

Latitude discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been erased and is no longer required or useful to Latitude operations or users. Latitude has server and computer hard drives destroyed by a local recycling company and receives a certificate of destruction for each retired hard drive. Paper, CDs, and DVDs are placed in locked bins at HQ and periodically shredded by a contracted disposal company.

System Operations Monitoring

The Latitude IT team monitors for known and new configuration and patching vulnerabilities through automated scans based on Qualys technology. IT reviews the vulnerability scan report, assesses the criticality of the vulnerabilities, and applies patches as applicable.

Security Violation Reporting and Monitoring

Latitude has established incident response procedures and centralized tracking tools, which consist of different channels for reporting production system incidents and weaknesses. Security and availability monitoring tools include Qualys, SEP, Salesforce, Azure, and M365. Incidents may also be reported via email by different Latitude teams or groups. The security teams operate 24x7x365 event/incident monitoring and response services.

Latitude has implemented incident response procedures, which consist of technical mechanisms, organizational infrastructure, and other procedures to detect, respond, and deter security incidents. The Latitude incident management technical infrastructure includes monitoring systems for detecting and alerting Latitude IT personnel of security events and incidents. A monitoring agent is installed on each server and computer at the time of server build-out to transfer the security logs to the central monitoring system, which identifies potential incidents and serves as a central repository for investigations. Incidents posing significant risk to the environment are prioritized for response and mitigation.

Change Management

Authorized Latitude users may view prior or upcoming upgrades and changes to the SubroChain® in the Salesforce SFDC issue log. In addition, Latitude customers receive notifications of major changes prior to change implementation through emails to active user accounts. Changes are identified via an IT helpdesk ticket from users or from IT support staff. These changes are discussed with management and if approved are entered into the Salesforce SFDC issue log for SubroChain® or IT HD ticket system for other systems.

The Latitude IT team monitors for known and new configuration and patching vulnerabilities through automated scans based on Qualys technology. IT reviews the vulnerability scan report from and assesses the criticality of the vulnerabilities and applies patches as applicable.

System Capacity Monitoring

Latitude IT team utilize different tools to monitor and evaluate their service's health (i.e., capacity, resiliency, and availability). These tools are configured to automatically alert assigned team members of issues impacting service health. The IT team monitors and resolves the issues that are reported or identified by providers. Salesforce is monitored by a web portal and major system interruptions are also automatically sent via email and text to IT members. M365 and Azure are monitored by tenant ID through online web portals. Any issue found during monitoring is communicated when appropriate to users or addressed through the normal change control process. Emergency capacity issues are addressed and approved by IT management for remediation. On an annual basis, LSS IT teams prepare an overview of the service team's capacity, availability, and resiliency from the prior year. This overview presents the root cause of anomalies or deviations to senior management and based on the meeting issues or changes to capacity and availability are tracked to resolution.

Environmental Security

Latitude monitors the computer room for temperature and humidity. Alerts are sent to IT staff when thresholds are exceeded. IT works with operations to resolves issues that are reported.

Backup and Recovery

SubroChain® and LCAP data is replicated for redundancy and disaster recovery purposes. SubroChain® data is replicated from the primary content database to a secondary content database within the same Salesforce instance/datacenter. The primary and secondary databases are then replicated across geographically dispersed datacenters to the Latitude data warehouse in Azure.

Generally, the data maintained in the primary content database is replicated and accessible in real time via:

(1) the primary database,

(2) a secondary replication database located in the same primary datacenter 2 - 4 times a year, and

(3) a secondary disaster recovery server with hourly replicated data in a geographically segregated datacenter

In addition to content replication and geographical redundancy, LSS LCAP data is also subject to a periodic Azure Blob Storage backup process. LCAP data is generally subject to two backup types, each with a unique cadence:

- Full Backups – Full backups consist of all customer content data on a server or content database, generally occur on a weekly frequency and are maintained for 30 days.
- Differential Backups – Differential backups occur at a daily frequency and consist of any additional data since the last full backup or differential backup, depending on which was the last to occur.

As data is accessible for redundancy and disaster recovery purposes for applications and support services through the data replication process described above, data backups are typically performed during the evenings in order not to interrupt operations.

Business Continuity and Disaster Recovery

Latitude performs periodic failover testing. Where relevant, failover exercises are conducted on a regular basis to test applications and related data to verify the accessibility at a secondary disaster recovery location. The frequency of conducting failover exercises, as well as the recovery time objectives (RTOs) for each application and support service, are based on the nature and criticality of the systems. The RTOs are developed as part of the overall M365 Business Continuity and Disaster Recovery Planning. The primary objective of conducting failover exercises is to test whether the RTOs could be met in the event of a cyber-attack, environmental event or similar disaster. Issues identified as part of the failover tests are tracked to ultimate resolution.

Information and Communications

Latitude has implemented various methods of communication to help provide assurance that all employees understand their individual roles and responsibilities and that significant events are communicated. These methods include orientation for new employees, training for all employees, and the use of e-mail messages to communicate time-sensitive information. Employees are encouraged to communicate with their lead/mentor, supervisor/manager or Senior/Executive Management.

Latitude has an information security policy to help ensure that employees understand their individual roles and responsibilities concerning processing and controls to ensure significant events are communicated in a timely manner. These include formal and informal training programs and the use of email to communicate time-sensitive information and processes for security and system availability purposes that notify key personnel in the event of problems.

Authorized Latitude users can view prior or upcoming upgrades and changes to the SubroChain® in the Salesforce SFDC issue log. In addition, Latitude customers receive notifications of major changes prior to change implementation through emails to active user accounts. Changes are identified via an IT helpdesk ticket from users or from IT support staff. These changes are discussed with management and if approved are entered into the Salesforce SFDC log for SubroChain® or IT HD ticket system for LCAP. SubroChain® users are notified of changes through Release Notes.

Latitude uses SharePoint, Revver, and SubroChain® to help facilitate the upload of user and client information, such as organization charts, client contacts, client workflows, and client complaints, to the appropriate repository in accordance with the client's contracted or workflow instructions.

Latitude has also implemented various methods of communication to help provide assurance that customers understand the roles and responsibilities in processing their transactions and communication of significant events. These methods include monthly meetings with representatives from all customers and the use of e-mail messages and our customer contact line to communicate time-sensitive information.

Monitoring Activities

To ensure the effectiveness of the controls to meet its service commitments and ensure the system is protected against unauthorized access, use, or modifications as well as uptime availability, LSS conducts a variety of monitoring activities. These activities include operational and system monitoring, dashboards and reports, ongoing assessments, and system reviews.

An owner is assigned to each enterprise risk as part of the Enterprise Risk Management Program. The risk owner assesses organizational and environmental factors and changes and the functioning of controls to identify and pursue improvements where needed. Work product quality reviews are used to monitor service results against best practices to help identify any problems so that corrective action and coaching can be implemented.

Additionally, subservice organizations are monitored through daily alerts of SaaS performance and outages as well as annual reviews of the subservice organization SOC 2® reports. Issues found in the SOC 2® reports or with monitored services are communicated to management and discussed to determine if corrective actions are needed.

CONTROL OBJECTIVES AND RELATED CONTROLS

Latitude's applicable trust services criteria and their related controls are included in Section 4, "Trust Services Criteria, Related Controls, and Test of Controls," to eliminate the redundancy that would result from listing them in this section and repeating them in Section 4. Although the control objectives and related controls are included in Section 4, they are, nevertheless, an integral part of Latitude's description of controls.

COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS

Latitude's controls related to the subrogation and salvage recovery services and vehicle material damage appraisal services system cover only a portion of overall internal control for each user entity of Latitude. Complementary controls at the subservice organizations are required to meet the applicable trust services criteria related to security and availability. Therefore, each user entity's internal control for security and availability must be evaluated in conjunction with Latitude's controls described in Section 4 of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organizations as described below.

Cloud Service Providers (**CSPs**) – Microsoft Azure, Salesforce Service Cloud, Microsoft365

Complementary Subservice Organization Controls	Applicable TSC
CSPs are responsible for protecting the transmission of client data within their environment.	5.2, 6.7
CSPs are responsible for implementing logical security controls within their systems and applications.	6.1, 6.2, 6.3, 6.6
CSPs are responsible for controlling and monitoring physical access to their facilities and data centers.	6.4, 7.2
CSPs are responsible for implementing network security controls within their operating environment to protect user entity data.	6.6
CSPs are responsible for maintaining and patching their applications and underlying environment.	8.1
CSPs are responsible for identifying, monitoring, evaluating and responding to events within their environments that could impact client systems and data.	7.1, 7.2, 7.3, 7.4 7.5
CSPs are responsible for a data center business continuity management that supports timely system recovery and availability.	7.5, 9.1, A1.1, A1.2, A1.3
CSPs are responsible for maintaining and monitoring environmental controls in their data centers.	A1.2
CSPs are responsible for automatically replicating customer data to minimize isolated faults.	A1.2

COMPLEMENTARY USER ENTITY CONTROLS

Latitude's controls related to the applicable trust services criteria for security and availability of the subrogation and salvage recovery services and vehicle material damage appraisal services system cover only a portion of overall internal control for each user entity of Latitude. Complementary controls at user entities are required to achieve the applicable trust services criteria for security and availability to be achieved solely by Latitude. Therefore, each user entity's internal control relative to security and availability should be evaluated in conjunction with Latitude's controls described in Section 4 of this report, taking into account the related complementary user entity controls associated with the relevant applicable trust services criteria, as indicated below.

In order for user entities to rely on the controls reported on herein, each user entity must evaluate its own internal control to determine whether the identified complementary user entity controls have been implemented and are operating effectively.

Complementary User Entity Controls	Applicable TSC
Client is responsible for using a secure method of transmittal for submitting data to Latitude.	6.7
Client is responsible for ensuring that only authorized and properly trained personnel are provided logical access to Latitude systems and reports, and notifying Latitude promptly when a user has been terminated or otherwise should no longer have access.	6.1, 6.2, 6.3
Customers are responsible for reporting security concerns and incidents to Latitude management in a timely manner.	2.3, 4.2
Application users are responsible for securing their user IDs and passwords used to access Latitude systems.	6.1, 6.2

Section 4:

Trust Services Criteria, Related Controls, and Tests of Controls

GUIDANCE REGARDING TESTS OF CONTROLS

When using information produced by the service organization, we evaluated whether the information was sufficiently reliable for our purposes, including, as necessary, obtaining evidence about the completeness and accuracy of the information and evaluating whether the information was sufficiently precise and detailed for our purposes.

The types of tests that may have been performed in evaluating the effectiveness of controls include inquiry, observation, inspection and/or re-performance.

APPLICABLE TRUST SERVICES CRITERIA

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

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 1	**Common Criteria Related to Control Environment**			
	Criteria	**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	3 Hiring Background Checks - Background checks, resume screening, and interviews are performed to evaluate the candidate's overall suitability and qualifications prior to their start date.	Inspected the new hire background checks, resume screening and interview notes for a sample of new hires to verify that management evaluated candidates' overall suitability and qualifications prior to their start date.	No exceptions noted.
		4 Employee Handbook - The Latitude Employee Handbook and the accompanying acknowledgement form sets expectations for employee conduct and treatment of confidential information. Acknowledgement from each employee is required upon hire and whenever the Handbook is revised.	Inspected the Latitude Employee Handbook to verify the Handbook set expectations for employee conduct and treatment of confidential information. Inspected the Latitude Employee Handbook acknowledgement forms for a sample of LSS new employees to verify that expectations for employee conduct and treatment of confidential information were acknowledged by the new employees. Inspected the Latitude Employee Handbook acknowledgement forms for a sample of LSS and IC employees to verify that expectations for employee conduct and treatment of confidential information were re-acknowledged by the employees when the Handbook was revised. Inquired with IC management and inspected the IC employee listing hire dates to verify there were no IC new hires during the period.	No exceptions noted with the Employee Handbook, LSS new hire acknowledgment process and LSS and IC employee annual re-acknowledgment process. Unable to verify the operating effectiveness of the IC new hire acknowledgment process because there were no IC new hires during the period.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 1	**Common Criteria Related to Control Environment**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		5 Performance Evaluations - Employee performance reviews are conducted within the new employee's probationary period and annually thereafter to ensure satisfactory performance, conduct and compliance with company requirements and standards.	Inspected the Employee Performance Review Policy to verify that performance reviews included an evaluation of an employee's performance, conduct and compliance with company requirements and standards. Inspected the performance reviews for a sample of LSS new employees to verify that management evaluated new employees' performance, conduct and compliance with company requirements and standards within the probationary period. Inspected the performance reviews for a sample of LSS and IC employees to verify that management evaluated employees' performance, conduct and compliance with company requirements and standards annually. Inquired with IC management and inspected the IC employee listing hire dates to verify there were no IC new hires during the period.	Exception noted on the employee annual performance reviews. For 1 of 3 (33.3%) IC employees, completion of the performance review was not tracked. See Management's Response in Section 5. No exceptions noted on the LSS new hire and annual performance reviews. Unable to verify the operating effectiveness of the IC new hire performance review process as there were no IC new hires during the period.
		6 Employee Discipline Process - A Disciplinary Action Policy is in place to provide progressive escalation and resolution of employee conduct to protect the best interests of the Company, its clients and employees.	Inspected the Disciplinary Action Policy to verify a policy was in place to provide progressive escalation and resolution of employee conduct to protect the best interests of the Company, its clients and employees.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 1	**Common Criteria Related to Control Environment**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	49 Exec Meetings - The Executive management team provides oversight and guidance on operational, technology and/or internal controls matters through monthly meetings and other communications.	Inspected the Executive meeting notices and presentations for a sample of months to verify Executive management provided oversight and guidance on operational, technology and/or internal controls matters.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	1 Company Organizational Design - The company is organized to provide clear accountability and authority, including separation of duties between subrogation, operations and IT functions.	Inspected the company organizational chart to verify the company was organized to provide clear accountability and authority and there was a separation of duties between subrogation, operations and IT functions.	No exceptions noted.
		53 Intranet Policies and Procedures - Policies and procedures for key activities are made available to employees on the company intranet to establish responsibilities and expectations for how work is to be completed.	Inspected the key policies and procedures on the Latitude intranet to verify policies and procedures were made available to employees to establish responsibilities and expectations for how work is to be completed.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	2 Job Descriptions - Job descriptions are in place to define roles and responsibilities as well as the educational and experience requirements for its personnel.	Inspected examples of job descriptions to verify job descriptions were in place to define roles and responsibilities and the educational and experience requirements for personnel.	No exceptions noted.
		3 Hiring Background Checks - Background checks, resume screening, and interviews are performed to evaluate the candidate's overall suitability and qualifications prior to their start date.	Inspected the new hire background checks, resume screening and interview notes for a sample of new hires to verify that management evaluated candidates' overall suitability and qualifications prior to their start date.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 1	**Common Criteria Related to Control Environment**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		5 Performance Evaluations - Employee performance reviews are conducted within the new employee's probationary period and annually thereafter to ensure satisfactory performance, conduct and compliance with company requirements and standards.	Inspected the Employee Performance Review Policy to verify that performance reviews included an evaluation of an employee's performance, conduct and compliance with company requirements and standards. Inspected the performance reviews for a sample of LSS new employees to verify that management evaluated new employees' performance, conduct and compliance with company requirements and standards within the probationary period. Inspected the performance reviews for a sample of LSS and IC employees to verify that management evaluated employees' performance, conduct and compliance with company requirements and standards annually. Inquired with IC management and inspected the IC employee listing hire dates to verify there were no IC new hires during the period.	Exception noted on the employee annual performance reviews. For 1 of 3 (33.3%) IC employees, completion of the performance review was not tracked. See Management's Response in Section 5. No exceptions noted on the LSS new hire and annual performance reviews. Unable to verify the operating effectiveness of the IC new hire performance review process as there were no IC new hires during the period.
		50 Claims Training - Claims training tailored to Latitude is available to all Latitude employees to improve their skills in representing clients during subrogation recovery efforts.	Inspected the Latitude Hub training page to verify Latitude-specific claims training was available to employees to improve their skills in representing clients during subrogation recovery efforts.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 1	**Common Criteria Related to Control Environment**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		55 Employee Engagement - Latitude creates an environment of employee engagement by providing benefits, and recognition activities in order to retain employees, build on their knowledge and expertise, and continually improve their effectiveness in fulfilling client activities.	Inspected the benefit enrollment announcement, Staff Turnover Risk Management Plan and examples of reward and recognition announcements to verify Latitude created an environment of employee engagement to develop and retain personnel.	No exceptions noted.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	2 Job Descriptions - Job descriptions are in place to define roles and responsibilities as well as the educational and experience requirements for its personnel.	Inspected examples of job descriptions to verify job descriptions were in place to define roles and responsibilities and the educational and experience requirements for personnel.	No exceptions noted.
		4 Employee Handbook - The Latitude Employee Handbook and the accompanying acknowledgement form sets expectations for employee conduct and treatment of confidential information. Acknowledgement from each employee is required upon hire and whenever the Handbook is revised.	Inspected the Latitude Employee Handbook to verify the Handbook set expectations for employee conduct and treatment of confidential information. Inspected the Latitude Employee Handbook acknowledgement forms for a sample of LSS new employees to verify that expectations for employee conduct and treatment of confidential information were acknowledged by the new employees. Inspected the Latitude Employee Handbook acknowledgement forms for a sample of LSS and IC employees to verify that expectations for employee conduct and treatment of confidential information were re-acknowledged by the employees when the Handbook was revised. Inquired with IC management and inspected the IC employee listing hire dates to verify there were no IC new hires during the period.	No exceptions noted with the Employee Handbook, LSS new hire acknowledgment process and LSS and IC employee annual re-acknowledgment process. Unable to verify the operating effectiveness of the IC new hire acknowledgment process because there were no IC new hires during the period.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 1	**Common Criteria Related to Control Environment**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		5 Performance Evaluations - Employee performance reviews are conducted within the new employee's probationary period and annually thereafter to ensure satisfactory performance, conduct and compliance with company requirements and standards.	Inspected the Employee Performance Review Policy to verify that performance reviews included an evaluation of an employee's performance, conduct and compliance with company requirements and standards. Inspected the performance reviews for a sample of LSS new employees to verify that management evaluated new employees' performance, conduct and compliance with company requirements and standards within the probationary period. Inspected the performance reviews for a sample of LSS and IC employees to verify that management evaluated employees' performance, conduct and compliance with company requirements and standards annually. Inquired with IC management and inspected the IC employee listing hire dates to verify there were no IC new hires during the period.	Exception noted on the employee annual performance reviews. For 1 of 3 (33.3%) IC employees, completion of the performance review was not tracked. See Management's Response in Section 5. No exceptions noted on the LSS new hire and annual performance reviews. Unable to verify the operating effectiveness of the IC new hire performance review process as there were no IC new hires during the period.
		6 Employee Discipline Process - A Disciplinary Action Policy is in place to provide progressive escalation and resolution of employee conduct to protect the best interests of the Company, its clients and employees.	Inspected the Disciplinary Action Policy to verify a policy was in place to provide progressive escalation and resolution of employee conduct to protect the best interests of the Company, its clients and employees.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 1	**Common Criteria Related to Control Environment**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		53 Intranet Policies and Procedures - Policies and procedures for key activities are made available to employees on the company intranet to establish responsibilities and expectations for how work is to be completed.	Inspected the key policies and procedures on the Latitude intranet to verify policies and procedures were made available to employees to establish responsibilities and expectations for how work is to be completed.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 2	**Common Criteria Related to Communication and Information**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	51 Performance Measures - Key performance metrics are generated and reviewed monthly by management to track the Subrogation and Salvage Specialists' performance quality and timeliness of client recoveries, and identify improvement opportunities for coaching.	Inspected the key performance reviews for a sample of months to verify key performance metrics were generated and reviewed monthly by management to track the Subrogation and Salvage Specialists' performance quality and timeliness of client recoveries, and identify improvement opportunities for coaching.	No exceptions noted.
		62 Client Feedback - Client feedback such as claim quality or service complaints are logged and tracked by the Business Development team through to resolution to ensure any issues are fully addressed.	Inspected the client feedback tracker to verify client feedback, including claim quality or service complaints, were logged and tracked by the Business Development team through to resolution to ensure any issues were fully addressed.	No exceptions noted.
		63 Dashboards - The SubroChain® claim handling system provides dashboards and reports to Specialists and management with operating results, activity completion status and cycle times, overall monitoring and alerts to help ensure the Company is operating as intended and to identify any exception situations requiring attention.	Observed the Subrogation Supervisor demonstrate the SubroChain® dashboards and reports that Specialists and Supervisors use to help them ensure the Company was operating as intended and identify exception situations requiring attention. Inspected examples of SubroChain® dashboards and reports to verify Specialists and Supervisors had access to operating results, activity completion status and cycle times, overall monitoring and alerts that help them ensure the Company is operating as intended and to identify exception situations requiring attention.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 2	**Common Criteria Related to Communication and Information**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		64 IT utilizes monitoring software on the network and LSS-controlled endpoints to identify and evaluate ongoing security threats and unusual system activity. Endpoints that are identified with an issue are either removed from operation or remedied in a timely manner.	Inspected the endpoint protection monitoring dashboard and screen shots of the software installed on the network and workstations to verify IT utilized monitoring software on the network and LSS-controlled endpoints to identify and evaluate ongoing security threats and unusual system activity. Inquired with IT management to verify there were no issues with endpoints during the period.	No exceptions noted on the monitoring software installed on the network and LSS-controlled endpoints to identify and evaluate ongoing security threats and unusual system activity. Unable to test the operating effectiveness of endpoint removals or remediation because there were no endpoints identified with an issue during the period.
		83 Vulnerability with pen testing is performed at least annually by a third party solution on the Latitude network, servers and web portal. Latitude management reviews the results and a remediation plan is developed, if necessary, to address any significant vulnerabilities.	Inspected the vulnerability with PEN test results to verify testing was performed at least annually on the Latitude network, servers and web portal. Inquired with IT management and inspected the results of the vulnerability with PEN test to verify there were no significant vulnerabilities identified during the period.	No exceptions noted with the annual vulnerability with PEN test. Unable to test the operating effectiveness of the remediation plan development and discussion with management because there were no significant vulnerabilities identified during the period.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 2	**Common Criteria Related to Communication and Information**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		86 Intrusion Detection / Protection System (IDS/IPS) software is used on all LSS endpoints to identify and protect against malicious network traffic. Alerts are monitored and reviewed by the LSS IT Team to resolve issues reported on the centralized dashboard.	Inspected screen shots of the IDS/IPS software installed on the network and workstations to verify IDS/IPS software was used on Latitude endpoints to identify and protect against malicious network traffic. Inspected the endpoint protection monitoring dashboard and examples of IDS/IPS alert emails sent to LSS IT to verify alerts were monitored and reviewed by the Latitude IT Team to resolve issues reported on the centralized dashboard.	No exceptions noted.
		106 IT management is notified when capacity issues for cloud-based, Latitude-controlled systems are detected. Additional capacity can be increased on demand as needed.	Inspected an example of a capacity notification and adjustment to verify IT management was notified when capacity issues for cloud-based, Latitude-controlled systems were detected and additional capacity could be increased on demand as needed.	No exceptions noted.
		108 Latitude's computer room is electronically monitored for temperature and humidity to protect the network equipment. Management is notified when temperature and humidity exceed pre-defined tolerance levels.	Inspected the environmental monitoring setting to verify Latitude's computer room was electronically monitored for temperature and humidity to protect the network equipment. Inspected the monitoring alert setting to verify thresholds were established and management was notified when temperature and humidity exceeded pre-defined tolerance levels.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 2	**Common Criteria Related to Communication and Information**			
	Criteria	**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	4 Employee Handbook - The Latitude Employee Handbook and the accompanying acknowledgement form sets expectations for employee conduct and treatment of confidential information. Acknowledgement from each employee is required upon hire and whenever the Handbook is revised.	Inspected the Latitude Employee Handbook to verify the Handbook set expectations for employee conduct and treatment of confidential information. Inspected the Latitude Employee Handbook acknowledgement forms for a sample of LSS new employees to verify that expectations for employee conduct and treatment of confidential information were acknowledged by the new employees. Inspected the Latitude Employee Handbook acknowledgement forms for a sample of LSS and IC employees to verify that expectations for employee conduct and treatment of confidential information were re-acknowledged by the employees when the Handbook was revised. Inquired with IC management and inspected the IC employee listing hire dates to verify there were no IC new hires during the period.	No exceptions noted with the Employee Handbook, LSS new hire acknowledgment process and LSS and IC employee annual re-acknowledgment process. Unable to verify the operating effectiveness of the IC new hire acknowledgment process because there were no IC new hires during the period.
		49 Exec Meetings - The Executive management team provides oversight and guidance on operational, technology and/or internal controls matters through monthly meetings and other communications.	Inspected the Executive meeting notices and presentations for a sample of months to verify Executive management provided oversight and guidance on operational, technology and/or internal controls matters.	No exceptions noted.
		54 Security Awareness Training - Security Awareness online training is assigned to all new Latitude employees as part of the onboarding process to ensure they are aware of security risks and how to mitigate them.	Inspected the Security Awareness online training log for a sample of new employees to verify security training and how to mitigate security risks was assigned to new employees as part of the onboarding process.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 2	**Common Criteria Related to Communication and Information**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		59 Changes made to the Client Access system that could impact the security and availability of the system are communicated via email to internal and external users who may be affected by the change.	Inquired of the Director of IT about the process for communicating Client Access system changes to internal and external users potentially affected by the change. Inquired with IT management and inspected the Client Access system log to verify there were no changes to the Client Access system during the period.	Unable to test the operating effectiveness of the Client Access system email communications because there were no Client Access system changes during the period.
		60 Release Notes - Release notes for every SubroChain® functional change are provided to all internal employees so that employees understand their responsibilities for using the system effectively.	Inspected the release notes for a sample of SubroChain® functional changes to verify release notes were provided to internal employees so that they understood their responsibilities for using the system effectively.	No exceptions noted.
		84 IT management conducts phishing campaigns to raise security awareness. Management identifies and follows up with users who require additional training or oversight.	Inspected the phishing campaign training tool and an example of a campaign to verify IT management conducted a phishing campaign to raise security awareness. Inspected an example of a training follow up email to verify Management identified and followed up with users who required additional training or oversight.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 2	**Common Criteria Related to Communication and Information**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		90 The Acceptable Use Policy establishes expectations for employees regarding the use of LSS information systems, and is acknowledged by employees upon hire and annually.	Inspected the Acceptable Use Policy to verify employee expectations regarding the use of Latitude information systems were established. Inspected the Acceptable Use Policy acknowledgement forms for a sample of LSS new employees to verify expectations regarding the use of LSS information systems were acknowledged by the LSS new employees upon hire. Inspected the Acceptable Use Policy acknowledgement forms for a sample of LSS and IC employees to verify expectations regarding the use of LSS information systems were re-acknowledged by employees annually. Inquired with IC management and inspected the IC employee listing hire dates to verify there were no IC new hires during the period.	No exceptions noted with the Acceptable Use Policy, LSS new hire acknowledgment process and employee annual re-acknowledgment process. Unable to verify the operating effectiveness of the IC new hire acknowledgment process because there were no IC new hires during the period.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	56 Client Contracts - Contracts are established with each client to outline the scope and mutual expectations for servicing work for the client.	Inspected the contract for a sample of clients to verify the contract outlined the scope and mutual expectations for servicing the client's work.	No exceptions noted.
		58 Client Communication - Clients have access to communication channels, such as the Client Access Portal and their Business Development team, to provide feedback, register issues or access information.	Inspected the Client Access Portal and examples of communications from the Business Development team to verify clients had access to communication channels to provide feedback, register issues or access information.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 2	**Common Criteria Related to Communication and Information**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		59 Changes made to the Client Access system that could impact the security and availability of the system are communicated via email to internal and external users who may be affected by the change.	Inquired of the Director of IT about the process for communicating Client Access system changes to internal and external users potentially affected by the change. Inquired with IT management and inspected the Client Access system log to verify there were no changes to the Client Access system during the period.	Unable to test the operating effectiveness of the Client Access system email communications because there were no Client Access system changes during the period.
		62 Client Feedback - Client feedback such as claim quality or service complaints are logged and tracked by the Business Development team through to resolution to ensure any issues are fully addressed.	Inspected the client feedback tracker to verify client feedback, including claim quality or service complaints, were logged and tracked by the Business Development team through to resolution to ensure any issues were fully addressed.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 3	**Common Criteria Related to Risk Assessment**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	16 Best Claim Practices - Management defined best claim practices (BCPs) to mitigate the risks inherent with subrogation for each line of business. The best practices are posted on the intranet to help guide subrogation teams in their subrogation claim handling activities.	Inspected examples of best claim practices (BCPs) to verify management defined BCPs to mitigate the risks inherent with subrogation for each line of business. Inspected a screen shot of the BCPs posted on the Company intranet to verify best practices were made available to help guide subrogation teams in their subrogation claim handling activities.	No exceptions noted.
		33 ERM - A strategic level risk assessment is completed by the executive team annually to identify, prioritize and track mitigation on the most important risks to the company, such as fraud or market risk. A risk owner is identified to assess and pursue improvements where needed.	Inspected the ERM Policy to verify a strategic level risk assessment process for identifying and prioritizing risks and developing mitigation plans was in place. Inspected the Risk Assessment spreadsheet to verify a strategic level risk assessment was completed by the executive team annually; risk mitigation activities for various risks were identified, prioritized, and tracked; and a risk owner was identified to assess and pursue improvements where needed.	No exceptions noted.
		34 Payment Fraud - The Finance Director and COO assess fraud risk over internal and external payment streams to ensure that sufficient controls have been established to prevent, detect or mitigate material fraudulent payments. Control improvements are identified and remediated and/or enhanced over time.	Inspected the Payment Fraud Risk and Control Plan to verify a plan was in place to assess fraud risk over internal and external payment streams to help prevent, detect or mitigate material fraudulent payments. Inspected the Risk Assessment spreadsheet to verify fraud risk was assessed by the Finance Director and COO, risks were remediated and control improvements were identified and/or enhanced.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 3	**Common Criteria Related to Risk Assessment**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**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.	33 ERM - A strategic level risk assessment is completed by the executive team annually to identify, prioritize and track mitigation on the most important risks to the company, such as fraud or market risk. A risk owner is identified to assess and pursue improvements where needed.	Inspected the ERM Policy to verify a strategic level risk assessment process for identifying and prioritizing risks and developing mitigation plans was in place. Inspected the Risk Assessment spreadsheet to verify a strategic level risk assessment was completed by the executive team annually; risk mitigation activities for various risks were identified, prioritized, and tracked; and a risk owner was identified to assess and pursue improvements where needed.	No exceptions noted.
		34 Payment Fraud - The Finance Director and COO assess fraud risk over internal and external payment streams to ensure that sufficient controls have been established to prevent, detect or mitigate material fraudulent payments. Control improvements are identified and remediated and/or enhanced over time.	Inspected the Payment Fraud Risk and Control Plan to verify a plan was in place to assess fraud risk over internal and external payment streams to help prevent, detect or mitigate material fraudulent payments. Inspected the Risk Assessment spreadsheet to verify fraud risk was assessed by the Finance Director and COO, risks were remediated and control improvements were identified and/or enhanced.	No exceptions noted.
		97 Annually, the IT Director reviews attestation reports for its SaaS and IaaS service providers to evaluate the effectiveness of controls critical to the operation of LSS's SubroChain® system. Deficiencies are reported and discussed in monthly SubroChain Steering Committee meetings to determine corrective course of action as needed.	Inspected the attestation report review presentations to verify the IT Director reviewed attestation reports for its SaaS and IaaS service providers, evaluated the effectiveness of controls critical to the operation of LSS's SubroChain® system, and reported and discussed deficiencies during the SubroChain Steering Committee meeting to determine any necessary corrective courses of action.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 3	**Common Criteria Related to Risk Assessment**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	33 ERM - A strategic level risk assessment is completed by the executive team annually to identify, prioritize and track mitigation on the most important risks to the company, such as fraud or market risk. A risk owner is identified to assess and pursue improvements where needed.	Inspected the ERM Policy to verify a strategic level risk assessment process for identifying and prioritizing risks and developing mitigation plans was in place. Inspected the Risk Assessment spreadsheet to verify a strategic level risk assessment was completed by the executive team annually; risk mitigation activities for various risks were identified, prioritized, and tracked; and a risk owner was identified to assess and pursue improvements where needed.	No exceptions noted.
		34 Payment Fraud - The Finance Director and COO assess fraud risk over internal and external payment streams to ensure that sufficient controls have been established to prevent, detect or mitigate material fraudulent payments. Control improvements are identified and remediated and/or enhanced over time.	Inspected the Payment Fraud Risk and Control Plan to verify a plan was in place to assess fraud risk over internal and external payment streams to help prevent, detect or mitigate material fraudulent payments. Inspected the Risk Assessment spreadsheet to verify fraud risk was assessed by the Finance Director and COO, risks were remediated and control improvements were identified and/or enhanced.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 3	**Common Criteria Related to Risk Assessment**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	33 ERM - A strategic level risk assessment is completed by the executive team annually to identify, prioritize and track mitigation on the most important risks to the company, such as fraud or market risk. A risk owner is identified to assess and pursue improvements where needed.	Inspected the ERM Policy to verify a strategic level risk assessment process for identifying and prioritizing risks and developing mitigation plans was in place. Inspected the Risk Assessment spreadsheet to verify a strategic level risk assessment was completed by the executive team annually; risk mitigation activities for various risks were identified, prioritized, and tracked; and a risk owner was identified to assess and pursue improvements where needed.	No exceptions noted.
		34 Payment Fraud - The Finance Director and COO assess fraud risk over internal and external payment streams to ensure that sufficient controls have been established to prevent, detect or mitigate material fraudulent payments. Control improvements are identified and remediated and/or enhanced over time.	Inspected the Payment Fraud Risk and Control Plan to verify a plan was in place to assess fraud risk over internal and external payment streams to help prevent, detect or mitigate material fraudulent payments. Inspected the Risk Assessment spreadsheet to verify fraud risk was assessed by the Finance Director and COO, risks were remediated and control improvements were identified and/or enhanced.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 4	**Common Criteria Related to Monitoring Activities**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**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.	63 Dashboards - The SubroChain® claim handling system provides dashboards and reports to Specialists and management with operating results, activity completion status and cycle times, overall monitoring and alerts to help ensure the Company is operating as intended and to identify any exception situations requiring attention.	Observed the Subrogation Supervisor demonstrate the SubroChain® dashboards and reports that Specialists and Supervisors use to help them ensure the Company was operating as intended and identify exception situations requiring attention. Inspected examples of SubroChain® dashboards and reports to verify Specialists and Supervisors had access to operating results, activity completion status and cycle times, overall monitoring and alerts that help them ensure the Company is operating as intended and to identify exception situations requiring attention.	No exceptions noted.
		64 IT utilizes monitoring software on the network and LSS-controlled endpoints to identify and evaluate ongoing security threats and unusual system activity. Endpoints that are identified with an issue are either removed from operation or remedied in a timely manner.	Inspected the endpoint protection monitoring dashboard and screen shots of the software installed on the network and workstations to verify IT utilized monitoring software on the network and LSS-controlled endpoints to identify and evaluate ongoing security threats and unusual system activity. Inquired with IT management to verify there were no issues with endpoints during the period.	No exceptions noted on the monitoring software installed on the network and LSS-controlled endpoints to identify and evaluate ongoing security threats and unusual system activity. Unable to test the operating effectiveness of endpoint removals or remediation because there were no endpoints identified with an issue during the period.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 4	**Common Criteria Related to Monitoring Activities**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		66 BCP - A Business Continuity Plan (BCP) is in place to help ensure timely resumption of critical business operations and systems in the event of various scenarios such as cyber attack, environmental event or similar disaster. The BCP is executed or tested at least annually and updated for lessons learned.	Inspected the Business Continuity Plan (BCP) to verify a plan was in place to help ensure timely resumption of critical business operations and systems in the event of various scenarios such as cyber attack, environmental event or similar disaster. Inspected the results of the BCP execution and plan updates to verify the BCP was executed or tested at least annually and updated for lessons learned.	No exceptions noted.
		76 IT reviews LSS system and application user accounts annually to assess appropriateness of role access and remove unused accounts so that only authorized users retain access.	Inspected the results of the annual user access review and examples of removed user accounts to verify IT reviewed LSS system and application user accounts annually to assess the appropriateness of role access and remove unused accounts so that only authorized users retained access.	No exceptions noted.
		83 Vulnerability with pen testing is performed at least annually by a third party solution on the Latitude network, servers and web portal. Latitude management reviews the results and a remediation plan is developed, if necessary, to address any significant vulnerabilities.	Inspected the vulnerability with PEN test results to verify testing was performed at least annually on the Latitude network, servers and web portal. Inquired with IT management and inspected the results of the vulnerability with PEN test to verify there were no significant vulnerabilities identified during the period.	No exceptions noted with the annual vulnerability with PEN test. Unable to test the operating effectiveness of the remediation plan development and discussion with management because there were no significant vulnerabilities identified during the period.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 4	**Common Criteria Related to Monitoring Activities**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		84 IT management conducts phishing campaigns to raise security awareness. Management identifies and follows up with users who require additional training or oversight.	Inspected the phishing campaign training tool and an example of a campaign to verify IT management conducted a phishing campaign to raise security awareness. Inspected an example of a training follow up email to verify Management identified and followed up with users who required additional training or oversight.	No exceptions noted.
		33 ERM - A strategic level risk assessment is completed by the executive team annually to identify, prioritize and track mitigation on the most important risks to the company, such as fraud or market risk. A risk owner is identified to assess and pursue improvements where needed.	Inspected the ERM Policy to verify a strategic level risk assessment process for identifying and prioritizing risks and developing mitigation plans was in place. Inspected the Risk Assessment spreadsheet to verify a strategic level risk assessment was completed by the executive team annually; risk mitigation activities for various risks were identified, prioritized, and tracked; and a risk owner was identified to assess and pursue improvements where needed.	No exceptions noted.
		34 Payment Fraud - The Finance Director and COO assess fraud risk over internal and external payment streams to ensure that sufficient controls have been established to prevent, detect or mitigate material fraudulent payments. Control improvements are identified and remediated and/or enhanced over time.	Inspected the Payment Fraud Risk and Control Plan to verify a plan was in place to assess fraud risk over internal and external payment streams to help prevent, detect or mitigate material fraudulent payments. Inspected the Risk Assessment spreadsheet to verify fraud risk was assessed by the Finance Director and COO, risks were remediated and control improvements were identified and/or enhanced.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 4	**Common Criteria Related to Monitoring Activities**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		97 Annually, the IT Director reviews attestation reports for its SaaS and IaaS service providers to evaluate the effectiveness of controls critical to the operation of LSS's SubroChain® system. Deficiencies are reported and discussed in monthly SubroChain Steering Committee meetings to determine corrective course of action as needed.	Inspected the attestation report review presentations to verify the IT Director reviewed attestation reports for its SaaS and IaaS service providers, evaluated the effectiveness of controls critical to the operation of LSS's SubroChain® system, and reported and discussed deficiencies during the SubroChain Steering Committee meeting to determine any necessary corrective courses of action.	No exceptions noted.
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.	63 Dashboards - The SubroChain® claim handling system provides dashboards and reports to Specialists and management with operating results, activity completion status and cycle times, overall monitoring and alerts to help ensure the Company is operating as intended and to identify any exception situations requiring attention.	Observed the Subrogation Supervisor demonstrate the SubroChain® dashboards and reports that Specialists and Supervisors use to help them ensure the Company was operating as intended and identify exception situations requiring attention. Inspected examples of SubroChain® dashboards and reports to verify Specialists and Supervisors had access to operating results, activity completion status and cycle times, overall monitoring and alerts that help them ensure the Company is operating as intended and to identify exception situations requiring attention.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 4	**Common Criteria Related to Monitoring Activities**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		83 Vulnerability with pen testing is performed at least annually by a third party solution on the Latitude network, servers and web portal. Latitude management reviews the results and a remediation plan is developed, if necessary, to address any significant vulnerabilities.	Inspected the vulnerability with PEN test results to verify testing was performed at least annually on the Latitude network, servers and web portal. Inquired with IT management and inspected the results of the vulnerability with PEN test to verify there were no significant vulnerabilities identified during the period.	No exceptions noted with the annual vulnerability with PEN test. Unable to test the operating effectiveness of the remediation plan development and discussion with management because there were no significant vulnerabilities identified during the period.
		84 IT management conducts phishing campaigns to raise security awareness. Management identifies and follows up with users who require additional training or oversight.	Inspected the phishing campaign training tool and an example of a campaign to verify IT management conducted a phishing campaign to raise security awareness. Inspected an example of a training follow up email to verify Management identified and followed up with users who required additional training or oversight.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 4	**Common Criteria Related to Monitoring Activities**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		33 ERM - A strategic level risk assessment is completed by the executive team annually to identify, prioritize and track mitigation on the most important risks to the company, such as fraud or market risk. A risk owner is identified to assess and pursue improvements where needed.	Inspected the ERM Policy to verify a strategic level risk assessment process for identifying and prioritizing risks and developing mitigation plans was in place. Inspected the Risk Assessment spreadsheet to verify a strategic level risk assessment was completed by the executive team annually; risk mitigation activities for various risks were identified, prioritized, and tracked; and a risk owner was identified to assess and pursue improvements where needed.	No exceptions noted.
		97 Annually, the IT Director reviews attestation reports for its SaaS and IaaS service providers to evaluate the effectiveness of controls critical to the operation of LSS's SubroChain® system. Deficiencies are reported and discussed in monthly SubroChain Steering Committee meetings to determine corrective course of action as needed.	Inspected the attestation report review presentations to verify the IT Director reviewed attestation reports for its SaaS and IaaS service providers, evaluated the effectiveness of controls critical to the operation of LSS's SubroChain® system, and reported and discussed deficiencies during the SubroChain Steering Committee meeting to determine any necessary corrective courses of action.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 5	**Common Criteria Related to Control Activities**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**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.	33 ERM - A strategic level risk assessment is completed by the executive team annually to identify, prioritize and track mitigation on the most important risks to the company, such as fraud or market risk. A risk owner is identified to assess and pursue improvements where needed.	Inspected the ERM Policy to verify a strategic level risk assessment process for identifying and prioritizing risks and developing mitigation plans was in place. Inspected the Risk Assessment spreadsheet to verify a strategic level risk assessment was completed by the executive team annually; risk mitigation activities for various risks were identified, prioritized, and tracked; and a risk owner was identified to assess and pursue improvements where needed.	No exceptions noted.
		34 Payment Fraud - The Finance Director and COO assess fraud risk over internal and external payment streams to ensure that sufficient controls have been established to prevent, detect or mitigate material fraudulent payments. Control improvements are identified and remediated and/or enhanced over time.	Inspected the Payment Fraud Risk and Control Plan to verify a plan was in place to assess fraud risk over internal and external payment streams to help prevent, detect or mitigate material fraudulent payments. Inspected the Risk Assessment spreadsheet to verify fraud risk was assessed by the Finance Director and COO, risks were remediated and control improvements were identified and/or enhanced.	No exceptions noted.
		97 Annually, the IT Director reviews attestation reports for its SaaS and IaaS service providers to evaluate the effectiveness of controls critical to the operation of LSS's SubroChain® system. Deficiencies are reported and discussed in monthly SubroChain Steering Committee meetings to determine corrective course of action as needed.	Inspected the attestation report review presentations to verify the IT Director reviewed attestation reports for its SaaS and IaaS service providers, evaluated the effectiveness of controls critical to the operation of LSS's SubroChain® system, and reported and discussed deficiencies during the SubroChain Steering Committee meeting to determine any necessary corrective courses of action.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 5	**Common Criteria Related to Control Activities**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	85 Firewall are in place to protect the Client Access system and to prevent unauthorized access to LSS networks. Only a limited number of System Administrators have access to make changes to the firewalls.	Inspected the firewall rules to verify firewalls were in place to protect the Client Access system and prevent unauthorized access to Latitude networks. Inspected list of firewall Administrators to verify only a limited number of System Administrators had access to make changes to the firewalls.	No exceptions noted.
		33 ERM - A strategic level risk assessment is completed by the executive team annually to identify, prioritize and track mitigation on the most important risks to the company, such as fraud or market risk. A risk owner is identified to assess and pursue improvements where needed.	Inspected the ERM Policy to verify a strategic level risk assessment process for identifying and prioritizing risks and developing mitigation plans was in place. Inspected the Risk Assessment spreadsheet to verify a strategic level risk assessment was completed by the executive team annually; risk mitigation activities for various risks were identified, prioritized, and tracked; and a risk owner was identified to assess and pursue improvements where needed.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 5	**Common Criteria Related to Control Activities**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		64 IT utilizes monitoring software on the network and LSS-controlled endpoints to identify and evaluate ongoing security threats and unusual system activity. Endpoints that are identified with an issue are either removed from operation or remedied in a timely manner.	Inspected the endpoint protection monitoring dashboard and screen shots of the software installed on the network and workstations to verify IT utilized monitoring software on the network and LSS-controlled endpoints to identify and evaluate ongoing security threats and unusual system activity. Inquired with IT management to verify there were no issues with endpoints during the period.	No exceptions noted on the monitoring software installed on the network and LSS-controlled endpoints to identify and evaluate ongoing security threats and unusual system activity. Unable to test the operating effectiveness of endpoint removals or remediation because there were no endpoints identified with an issue during the period.
		65 Endpoint Protection software is installed to protect the LSS-controlled servers and workstations from malicious code or viruses. The software is automatically updated for new threat definitions.	Inspected the endpoint protection monitoring dashboard and screen shots of the software installed on the network and workstations to verify endpoint protection software was installed to protect the LSS-controlled servers and workstations from malicious code or viruses. Inspected the software threat update configuration to verify the endpoint protection software was automatically updated for new threat definitions.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 5	**Common Criteria Related to Control Activities**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		86 Intrusion Detection / Protection System (IDS/IPS) software is used on all LSS endpoints to identify and protect against malicious network traffic. Alerts are monitored and reviewed by the LSS IT Team to resolve issues reported on the centralized dashboard.	Inspected screen shots of the IDS/IPS software installed on the network and workstations to verify IDS/IPS software was used on Latitude endpoints to identify and protect against malicious network traffic. Inspected the endpoint protection monitoring dashboard and examples of IDS/IPS alert emails sent to LSS IT to verify alerts were monitored and reviewed by the Latitude IT Team to resolve issues reported on the centralized dashboard.	No exceptions noted.
		105 Security patches on Latitude-controlled endpoints and servers are applied monthly or as needed based on criticality to enhance performance and protect systems from vulnerabilities.	Inspected examples of security patches applied to Latitude-controlled endpoints and servers to verify security patches were applied monthly or as needed based on criticality to enhance performance and protect systems from vulnerabilities.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	2 Job Descriptions - Job descriptions are in place to define roles and responsibilities as well as the educational and experience requirements for its personnel.	Inspected examples of job descriptions to verify job descriptions were in place to define roles and responsibilities and the educational and experience requirements for personnel.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 5	**Common Criteria Related to Control Activities**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		4 Employee Handbook - The Latitude Employee Handbook and the accompanying acknowledgement form sets expectations for employee conduct and treatment of confidential information. Acknowledgement from each employee is required upon hire and whenever the Handbook is revised.	Inspected the Latitude Employee Handbook to verify the Handbook set expectations for employee conduct and treatment of confidential information. Inspected the Latitude Employee Handbook acknowledgement forms for a sample of LSS new employees to verify that expectations for employee conduct and treatment of confidential information were acknowledged by the new employees. Inspected the Latitude Employee Handbook acknowledgement forms for a sample of LSS and IC employees to verify that expectations for employee conduct and treatment of confidential information were re-acknowledged by the employees when the Handbook was revised. Inquired with IC management and inspected the IC employee listing hire dates to verify there were no IC new hires during the period.	No exceptions noted with the Employee Handbook, LSS new hire acknowledgment process and LSS and IC employee annual re-acknowledgment process. Unable to verify the operating effectiveness of the IC new hire acknowledgment process because there were no IC new hires during the period.
		53 Intranet Policies And Procedures - Policies and procedures for key activities are made available to employees on the company intranet to establish responsibilities and expectations for how work is to be completed.	Inspected the key policies and procedures on the Latitude intranet to verify policies and procedures were made available to employees to establish responsibilities and expectations for how work is to be completed.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 5	**Common Criteria Related to Control Activities**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		67 An Incident Response Policy is in place to guide in identifying, responding to, and mitigating both electronic and physical security incidents. The IT Director reviews and updates the Policy as needed for changes to the process.	Inspected the Incident Response Policy to verify a plan was in place to guide in identifying, responding to, and mitigating both electronic and physical security incidents. Inspected the Incident Response Policy version history to verify the IT Director reviewed and updated the Policy as needed for changes to the process.	No exceptions noted.
		90 The Acceptable Use Policy establishes expectations for employees regarding the use of LSS information systems, and is acknowledged by employees upon hire and annually.	Inspected the Acceptable Use Policy to verify employee expectations regarding the use of Latitude information systems were established. Inspected the Acceptable Use Policy acknowledgement forms for a sample of LSS new employees to verify expectations regarding the use of LSS information systems were acknowledged by the LSS new employees upon hire. Inspected the Acceptable Use Policy acknowledgement forms for a sample of LSS and IC employees to verify expectations regarding the use of LSS information systems were re-acknowledged by employees annually. Inquired with IC management and inspected the IC employee listing hire dates to verify there were no IC new hires during the period.	No exceptions noted with the Acceptable Use Policy, LSS new hire acknowledgment process and employee annual re-acknowledgment process. Unable to verify the operating effectiveness of the IC new hire acknowledgment process because there were no IC new hires during the period.
		91 Management maintains formal policies for data encryption, retention, duplication, and destruction in accordance with confidentiality commitments.	Inspected the data management policies to verify management maintained formal policies for data encryption, retention, duplication, and destruction in accordance with confidentiality commitments.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 5	**Common Criteria Related to Control Activities**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		16 Best Claim Practices - Management defined best claim practices (BCPs) to mitigate the risks inherent with subrogation for each line of business. The best practices are posted on the intranet to help guide subrogation teams in their subrogation claim handling activities.	Inspected examples of best claim practices (BCPs) to verify management defined BCPs to mitigate the risks inherent with subrogation for each line of business. Inspected a screen shot of the BCPs posted on the Company intranet to verify best practices were made available to help guide subrogation teams in their subrogation claim handling activities.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 6	**Common Criteria Related to Logical and Physical Access Controls**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**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.	71 User access to LSS systems and applications requires a unique user ID and password. Password settings for LSS controlled systems and applications are configured to enforce minimum password length, password complexity and/or periodic password rotations.	Inspected the LSS system and application password settings to verify passwords for LSS controlled systems and applications were configured to enforce minimum password length, password complexity and/or periodic password rotations. Observed the Director of Information Technology log in to the LSS systems and applications to verify user access to required a unique user ID and password.	No exceptions noted.
		72 Employee access to M365, SubroChain®, and IC Claims Tracker requires multi-factor authentication to increase access security.	Observed the Director of Information Technology access M365, SubroChain®, and IC Claims Tracker to verify employee access required multi-factor authentication for increased access security.	No exceptions noted.
		77 Client users are restricted to their own file storage containing their reports using their unique company identifier. In order to access their reports, clients authenticate to the Client Access Portal using their unique user ID and passcode.	Observed the Director of Information Technology access the Client Access Portal to verify access to the Client Access Portal required a unique user ID and passcode. Observed the Director of Information Technology demonstrate the client access restrictions in the Client Access Portal to verify client users were restricted to their own file storage using their unique company identifier.	No exceptions noted.
		85 Firewall are in place to protect the Client Access system and to prevent unauthorized access to LSS networks. Only a limited number of System Administrators have access to make changes to the firewalls.	Inspected the firewall rules to verify firewalls were in place to protect the Client Access system and prevent unauthorized access to Latitude networks. Inspected list of firewall Administrators to verify only a limited number of System Administrators had access to make changes to the firewalls.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 6	**Common Criteria Related to Logical and Physical Access Controls**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		73 A role-based access control (RBAC) matrix, security groups and an Employee Onboarding Checklist are utilized to set up new employee access to LSS systems and applications. Access to systems and assigned permissions are based on the principle of least privileges. Additional access or access changes are approved by the user's supervisors prior to access being provisioned.	Inspected the role-based access control (RBAC) matrices and security groups to verify an RBAC matrix and security groups were utilized in the process of setting up new employee access to LSS systems and applications, and permissions were assigned based on the principle of least privileges. Inspected the Employee Onboarding Checklist for a sample of LSS new employees to verify an Employee Onboarding Checklist was utilized to set up access to LSS systems and applications. Inspected the approvals for a sample of SubroChain® access changes during the period January 1, 2023 to March 31, 2023 to verify access was approved by the user's supervisor prior to access being provisioned.	Exception noted on the SubroChain® access change documentation. The SubroChain® listing of user access changes between April 1, 2022 - December 31, 2022 was not available due to system limitations. See Management's Response in Section 5. No exceptions noted with the RBAC matrices, security groups or SubroChain® access changes during the period January 1, 2023 to March 31, 2023.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 6	**Common Criteria Related to Logical and Physical Access Controls**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**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.	73 A role-based access control (RBAC) matrix, security groups and an Employee Onboarding Checklist are utilized to set up new employee access to LSS systems and applications. Access to systems and assigned permissions are based on the principle of least privileges. Additional access or access changes are approved by the user's supervisors prior to access being provisioned.	Inspected the role-based access control (RBAC) matrices and security groups to verify an RBAC matrix and security groups were utilized in the process of setting up new employee access to LSS systems and applications, and permissions were assigned based on the principle of least privileges. Inspected the Employee Onboarding Checklist for a sample of LSS new employees to verify an Employee Onboarding Checklist was utilized to set up access to LSS systems and applications. Inspected the approvals for a sample of SubroChain® access changes during the period January 1, 2023 to March 31, 2023 to verify access was approved by the user's supervisor prior to access being provisioned.	Exception noted on the SubroChain® access change documentation. The SubroChain® listing of user access changes between April 1, 2022 - December 31, 2022 was not available due to system limitations. See Management's Response in Section 5. No exceptions noted with the RBAC matrices, security groups or SubroChain® access changes during the period January 1, 2023 to March 31, 2023.
		75 HR completes an Employee Departure Checklist to ensure requests for removal of system access and physical access to the Latitude Corporate Office is not overlooked. Once notified, IT disables access in a timely manner.	Inspected the Employee Departure Checklists for a sample of LSS and IC terminated employees to verify removal of system access was not overlooked and IT disabled terminated employees' system access in a timely manner once notified.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 6	**Common Criteria Related to Logical and Physical Access Controls**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		76 IT reviews LSS system and application user accounts annually to assess appropriateness of role access and remove unused accounts so that only authorized users retain access.	Inspected the results of the annual user access review and examples of removed user accounts to verify IT reviewed LSS system and application user accounts annually to assess the appropriateness of role access and remove unused accounts so that only authorized users retained access.	No exceptions noted.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	73 A role-based access control (RBAC) matrix, security groups and an Employee Onboarding Checklist are utilized to set up new employee access to LSS systems and applications. Access to systems and assigned permissions are based on the principle of least privileges. Additional access or access changes are approved by the user's supervisors prior to access being provisioned.	Inspected the role-based access control (RBAC) matrices and security groups to verify an RBAC matrix and security groups were utilized in the process of setting up new employee access to LSS systems and applications, and permissions were assigned based on the principle of least privileges. Inspected the Employee Onboarding Checklist for a sample of LSS new employees to verify an Employee Onboarding Checklist was utilized to set up access to LSS systems and applications. Inspected the approvals for a sample of SubroChain® access changes during the period January 1, 2023 to March 31, 2023 to verify access was approved by the user's supervisor prior to access being provisioned.	Exception noted on the SubroChain® access change documentation. The SubroChain® listing of user access changes between April 1, 2022 - December 31, 2022 was not available due to system limitations. See Management's Response in Section 5. No exceptions noted with the RBAC matrices, security groups or SubroChain® access changes during the period January 1, 2023 to March 31, 2023.
		75 HR completes an Employee Departure Checklist to ensure requests for removal of system access and physical access to the Latitude Corporate Office is not overlooked. Once notified, IT disables access in a timely manner.	Inspected the Employee Departure Checklists for a sample of LSS and IC terminated employees to verify removal of system access was not overlooked and IT disabled terminated employees' system access in a timely manner once notified.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 6	**Common Criteria Related to Logical and Physical Access Controls**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		76 IT reviews LSS system and application user accounts annually to assess appropriateness of role access and remove unused accounts so that only authorized users retain access.	Inspected the results of the annual user access review and examples of removed user accounts to verify IT reviewed LSS system and application user accounts annually to assess the appropriateness of role access and remove unused accounts so that only authorized users retained access.	No exceptions noted.
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.	75 HR completes an Employee Departure Checklist to ensure requests for removal of system access and physical access to the Latitude Corporate Office is not overlooked. Once notified, IT disables access in a timely manner.	Inquired with the LSS Director of Operations and IC Director of Specialty Operations that no IC employees have physical access to the Latitude Corporate office. Inspected the Employee Departure Checklists for a sample of LSS terminated employees to verify removal of physical access to the Latitude Corporate Office was not overlooked and IT disabled the terminated LSS employees' physical access in a timely manner once notified.	Exceptions noted on the physical access removals for LSS terminated employees. For 2 of 2 (100%) LSS terminated employees with physical access to the corporate office, documentation showing HR completed an Employee Departure Checklist and IT removed physical access could not be provided. See Management's Response in Section 5.
		87 Access to the corporate facility is controlled by biometric locks. Access is monitored by an alarm system on entry points and video surveillance throughout the office.	Observed the biometric locks and alarm system during a virtual walk through of the Latitude office suite to verify access to the corporate facility was controlled by biometric locks, entry points were monitored by an alarm system and video surveillance was located throughout the office.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 6	**Common Criteria Related to Logical and Physical Access Controls**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		89 Access to the LSS server room is controlled by a biometric lock. Access is restricted to a limited number of appropriate personnel.	Observed the biometric locking device during a virtual walk through of the Latitude office suite to verify access to the server room was controlled by a biometric lock. Inspected the list of employees with access to Latitude's server room to verify access was restricted to a limited number of appropriate personnel.	No exceptions noted.
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.	78 Discarded client confidential information is secured in locked bins until disposed of by a contracted shredding service.	Observed the locked bin during a virtual walk through of the Latitude office suite with the Director of Information Technology to verify discarded client confidential information was secured. Inspected the shredding service's invoices to verify discarded client confidential information was disposed of by a contracted shredding service.	No exceptions noted.
		79 A third party vendor is utilized to erase/destroy computer hard drives. A Certificate of Destruction is provided by the third part as evidence of data destruction.	Inspected the certificate of destruction to verify a third party vendor was utilized to erase/destroy computer hard drives.	No exceptions noted.
		91 Management maintains formal policies for data encryption, retention, duplication, and destruction in accordance with confidentiality commitments.	Inspected the data management policies to verify management maintained formal policies for data encryption, retention, duplication, and destruction in accordance with confidentiality commitments.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 6	**Common Criteria Related to Logical and Physical Access Controls**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	72 Employee access to M365, SubroChain®, and IC Claims Tracker requires multi-factor authentication to increase access security.	Observed the Director of Information Technology access M365, SubroChain®, and IC Claims Tracker to verify employee access required multi-factor authentication for increased access security.	No exceptions noted.
		81 Latitude's customer data stored in the cloud-hosted Salesforce, AWS and Azure environments is encrypted at rest.	Inspected the cloud-hosted product information to verify Latitude's customer data stored in Salesforce, AWS and Azure environments was encrypted at rest.	No exceptions noted.
		82 IT disables the use of USB ports on Company-owned computers to prevent non-administrative users from installing unauthorized or malicious software and restrict removal of information.	Inspected the desktop configuration to verify IT disabled the use of USB ports on Company-owned computers to prevent non-administrative users from installing unauthorized or malicious software and restrict removal of information.	No exceptions noted.
		85 Firewall are in place to protect the Client Access system and to prevent unauthorized access to LSS networks. Only a limited number of System Administrators have access to make changes to the firewalls.	Inspected the firewall rules to verify firewalls were in place to protect the Client Access system and prevent unauthorized access to Latitude networks. Inspected list of firewall Administrators to verify only a limited number of System Administrators had access to make changes to the firewalls.	No exceptions noted.
		86 Intrusion Detection / Protection System (IDS/IPS) software is used on all LSS endpoints to identify and protect against malicious network traffic. Alerts are monitored and reviewed by the LSS IT Team to resolve issues reported on the centralized dashboard.	Inspected screen shots of the IDS/IPS software installed on the network and workstations to verify IDS/IPS software was used on Latitude endpoints to identify and protect against malicious network traffic. Inspected the endpoint protection monitoring dashboard and examples of IDS/IPS alert emails sent to LSS IT to verify alerts were monitored and reviewed by the Latitude IT Team to resolve issues reported on the centralized dashboard.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 6	**Common Criteria Related to Logical and Physical Access Controls**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		65 Endpoint Protection software is installed to protect the LSS-controlled servers and workstations from malicious code or viruses. The software is automatically updated for new threat definitions.	Inspected the endpoint protection monitoring dashboard and screen shots of the software installed on the network and workstations to verify endpoint protection software was installed to protect the LSS-controlled servers and workstations from malicious code or viruses. Inspected the software threat update configuration to verify the endpoint protection software was automatically updated for new threat definitions.	No exceptions noted.
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.	78 Discarded client confidential information is secured in locked bins until disposed of by a contracted shredding service.	Observed the locked bin during a virtual walk through of the Latitude office suite with the Director of Information Technology to verify discarded client confidential information was secured. Inspected the shredding service's invoices to verify discarded client confidential information was disposed of by a contracted shredding service.	No exceptions noted.
		79 A third party vendor is utilized to erase/destroy computer hard drives. A Certificate of Destruction is provided by the third part as evidence of data destruction.	Inspected the certificate of destruction to verify a third party vendor was utilized to erase/destroy computer hard drives.	No exceptions noted.
		80 A secure file sharing web portal or secure FTP (SFTP) site are availllable for transmission of confidential and/or sensitive information over public networks.	Inspected the web portal and SFTP site transmission security settings to verify secure mechanisms were available for transmitting confidential and/or sensitive information over public networks.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 6	**Common Criteria Related to Logical and Physical Access Controls**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		82 IT disables the use of USB ports on Company-owned computers to prevent non-administrative users from installing unauthorized or malicious software and restrict removal of information.	Inspected the desktop configuration to verify IT disabled the use of USB ports on Company-owned computers to prevent non-administrative users from installing unauthorized or malicious software and restrict removal of information.	No exceptions noted.
		91 Management maintains formal policies for data encryption, retention, duplication, and destruction in accordance with confidentiality commitments.	Inspected the data management policies to verify management maintained formal policies for data encryption, retention, duplication, and destruction in accordance with confidentiality commitments.	No exceptions noted.
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.	64 IT utilizes monitoring software on the network and LSS-controlled endpoints to identify and evaluate ongoing security threats and unusual system activity. Endpoints that are identified with an issue are either removed from operation or remedied in a timely manner.	Inspected the endpoint protection monitoring dashboard and screen shots of the software installed on the network and workstations to verify IT utilized monitoring software on the network and LSS-controlled endpoints to identify and evaluate ongoing security threats and unusual system activity. Inquired with IT management to verify there were no issues with endpoints during the period.	No exceptions noted on the monitoring software installed on the network and LSS-controlled endpoints to identify and evaluate ongoing security threats and unusual system activity. Unable to test the operating effectiveness of endpoint removals or remediation because there were no endpoints identified with an issue during the period.
		82 IT disables the use of USB ports on Company-owned computers to prevent non-administrative users from installing unauthorized or malicious software and restrict removal of information.	Inspected the desktop configuration to verify IT disabled the use of USB ports on Company-owned computers to prevent non-administrative users from installing unauthorized or malicious software and restrict removal of information.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 6	**Common Criteria Related to Logical and Physical Access Controls**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		83 Vulnerability with pen testing is performed at least annually by a third party solution on the Latitude network, servers and web portal. Latitude management reviews the results and a remediation plan is developed, if necessary, to address any significant vulnerabilities.	Inspected the vulnerability with PEN test results to verify testing was performed at least annually on the Latitude network, servers and web portal. Inquired with IT management and inspected the results of the vulnerability with PEN test to verify there were no significant vulnerabilities identified during the period.	No exceptions noted with the annual vulnerability with PEN test. Unable to test the operating effectiveness of the remediation plan development and discussion with management because there were no significant vulnerabilities identified during the period.
		84 IT management conducts phishing campaigns to raise security awareness. Management identifies and follows up with users who require additional training or oversight.	Inspected the phishing campaign training tool and an example of a campaign to verify IT management conducted a phishing campaign to raise security awareness. Inspected an example of a training follow up email to verify Management identified and followed up with users who required additional training or oversight.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 6	**Common Criteria Related to Logical and Physical Access Controls**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		86 Intrusion Detection / Protection System (IDS/IPS) software is used on all LSS endpoints to identify and protect against malicious network traffic. Alerts are monitored and reviewed by the LSS IT Team to resolve issues reported on the centralized dashboard.	Inspected screen shots of the IDS/IPS software installed on the network and workstations to verify IDS/IPS software was used on Latitude endpoints to identify and protect against malicious network traffic. Inspected the endpoint protection monitoring dashboard and examples of IDS/IPS alert emails sent to LSS IT to verify alerts were monitored and reviewed by the Latitude IT Team to resolve issues reported on the centralized dashboard.	No exceptions noted.
		65 Endpoint Protection software is installed to protect the LSS-controlled servers and workstations from malicious code or viruses. The software is automatically updated for new threat definitions.	Inspected the endpoint protection monitoring dashboard and screen shots of the software installed on the network and workstations to verify endpoint protection software was installed to protect the LSS-controlled servers and workstations from malicious code or viruses. Inspected the software threat update configuration to verify the endpoint protection software was automatically updated for new threat definitions.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 7	**Common Criteria Related to System Operations**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	64 IT utilizes monitoring software on the network and LSS-controlled endpoints to identify and evaluate ongoing security threats and unusual system activity. Endpoints that are identified with an issue are either removed from operation or remedied in a timely manner.	Inspected the endpoint protection monitoring dashboard and screen shots of the software installed on the network and workstations to verify IT utilized monitoring software on the network and LSS-controlled endpoints to identify and evaluate ongoing security threats and unusual system activity. Inquired with IT management to verify there were no issues with endpoints during the period.	No exceptions noted on the monitoring software installed on the network and LSS-controlled endpoints to identify and evaluate ongoing security threats and unusual system activity. Unable to test the operating effectiveness of endpoint removals or remediation because there were no endpoints identified with an issue during the period.
		65 Endpoint Protection software is installed to protect the LSS-controlled servers and workstations from malicious code or viruses. The software is automatically updated for new threat definitions.	Inspected the endpoint protection monitoring dashboard and screen shots of the software installed on the network and workstations to verify endpoint protection software was installed to protect the LSS-controlled servers and workstations from malicious code or viruses. Inspected the software threat update configuration to verify the endpoint protection software was automatically updated for new threat definitions.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 7	**Common Criteria Related to System Operations**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		83 Vulnerability with pen testing is performed at least annually by a third party solution on the Latitude network, servers and web portal. Latitude management reviews the results and a remediation plan is developed, if necessary, to address any significant vulnerabilities.	Inspected the vulnerability with PEN test results to verify testing was performed at least annually on the Latitude network, servers and web portal. Inquired with IT management and inspected the results of the vulnerability with PEN test to verify there were no significant vulnerabilities identified during the period.	No exceptions noted with the annual vulnerability with PEN test. Unable to test the operating effectiveness of the remediation plan development and discussion with management because there were no significant vulnerabilities identified during the period.
		85 Firewall are in place to protect the Client Access system and to prevent unauthorized access to LSS networks. Only a limited number of System Administrators have access to make changes to the firewalls.	Inspected the firewall rules to verify firewalls were in place to protect the Client Access system and prevent unauthorized access to Latitude networks. Inspected list of firewall Administrators to verify only a limited number of System Administrators had access to make changes to the firewalls.	No exceptions noted.
		86 Intrusion Detection / Protection System (IDS/IPS) software is used on all LSS endpoints to identify and protect against malicious network traffic. Alerts are monitored and reviewed by the LSS IT Team to resolve issues reported on the centralized dashboard.	Inspected screen shots of the IDS/IPS software installed on the network and workstations to verify IDS/IPS software was used on Latitude endpoints to identify and protect against malicious network traffic. Inspected the endpoint protection monitoring dashboard and examples of IDS/IPS alert emails sent to LSS IT to verify alerts were monitored and reviewed by the Latitude IT Team to resolve issues reported on the centralized dashboard.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 7	**Common Criteria Related to System Operations**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**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.	64 IT utilizes monitoring software on the network and LSS-controlled endpoints to identify and evaluate ongoing security threats and unusual system activity. Endpoints that are identified with an issue are either removed from operation or remedied in a timely manner.	Inspected the endpoint protection monitoring dashboard and screen shots of the software installed on the network and workstations to verify IT utilized monitoring software on the network and LSS-controlled endpoints to identify and evaluate ongoing security threats and unusual system activity. Inquired with IT management to verify there were no issues with endpoints during the period.	No exceptions noted on the monitoring software installed on the network and LSS-controlled endpoints to identify and evaluate ongoing security threats and unusual system activity. Unable to test the operating effectiveness of endpoint removals or remediation because there were no endpoints identified with an issue during the period.
		68 Subrogation and claims data backups for LSS systems and applications are performed on a scheduled basis. The completion of backups are monitored by the IT System Administrator for successful completion. Backup job failures are rerun the next business day.	Inspected the backup jobs, schedules and results of backups to verify subrogation and claims data backups for LSS systems and applications were performed on a scheduled basis. Inspected the backup alert notification configuration to verify the IT System Administrator monitored the completion of backups for successful completion. Inquired with IT management and inspected the backup log to verify there were no failed backups during the period.	No exceptions noted on the backup job schedules and monitoring. Unable to test the operating effectiveness of backup job failure reruns because there were no failed backups during the period.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 7	**Common Criteria Related to System Operations**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		86 Intrusion Detection / Protection System (IDS/IPS) software is used on all LSS endpoints to identify and protect against malicious network traffic. Alerts are monitored and reviewed by the LSS IT Team to resolve issues reported on the centralized dashboard.	Inspected screen shots of the IDS/IPS software installed on the network and workstations to verify IDS/IPS software was used on Latitude endpoints to identify and protect against malicious network traffic. Inspected the endpoint protection monitoring dashboard and examples of IDS/IPS alert emails sent to LSS IT to verify alerts were monitored and reviewed by the Latitude IT Team to resolve issues reported on the centralized dashboard.	No exceptions noted.
		106 IT management is notified when capacity issues for cloud-based, Latitude-controlled systems are detected. Additional capacity can be increased on demand as needed.	Inspected an example of a capacity notification and adjustment to verify IT management was notified when capacity issues for cloud-based, Latitude-controlled systems were detected and additional capacity could be increased on demand as needed.	No exceptions noted.
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.	64 IT utilizes monitoring software on the network and LSS-controlled endpoints to identify and evaluate ongoing security threats and unusual system activity. Endpoints that are identified with an issue are either removed from operation or remedied in a timely manner.	Inspected the endpoint protection monitoring dashboard and screen shots of the software installed on the network and workstations to verify IT utilized monitoring software on the network and LSS-controlled endpoints to identify and evaluate ongoing security threats and unusual system activity. Inquired with IT management to verify there were no issues with endpoints during the period.	No exceptions noted on the monitoring software installed on the network and LSS-controlled endpoints to identify and evaluate ongoing security threats and unusual system activity. Unable to test the operating effectiveness of endpoint removals or remediation because there were no endpoints identified with an issue during the period.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 7	**Common Criteria Related to System Operations**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		67 An Incident Response Policy is in place to guide in identifying, responding to, and mitigating both electronic and physical security incidents. The IT Director reviews and updates the Policy as needed for changes to the process.	Inspected the Incident Response Policy to verify a plan was in place to guide in identifying, responding to, and mitigating both electronic and physical security incidents. Inspected the Incident Response Policy version history to verify the IT Director reviewed and updated the Policy as needed for changes to the process.	No exceptions noted.
		86 Intrusion Detection / Protection System (IDS/IPS) software is used on all LSS endpoints to identify and protect against malicious network traffic. Alerts are monitored and reviewed by the LSS IT Team to resolve issues reported on the centralized dashboard.	Inspected screen shots of the IDS/IPS software installed on the network and workstations to verify IDS/IPS software was used on Latitude endpoints to identify and protect against malicious network traffic. Inspected the endpoint protection monitoring dashboard and examples of IDS/IPS alert emails sent to LSS IT to verify alerts were monitored and reviewed by the Latitude IT Team to resolve issues reported on the centralized dashboard.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	66 BCP - A Business Continuity Plan (BCP) is in place to help ensure timely resumption of critical business operations and systems in the event of various scenarios such as cyber attack, environmental event or similar disaster. The BCP is executed or tested at least annually and updated for lessons learned.	Inspected the Business Continuity Plan (BCP) to verify a plan was in place to help ensure timely resumption of critical business operations and systems in the event of various scenarios such as cyber attack, environmental event or similar disaster. Inspected the results of the BCP execution and plan updates to verify the BCP was executed or tested at least annually and updated for lessons learned.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 7	**Common Criteria Related to System Operations**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		67 An Incident Response Policy is in place to guide in identifying, responding to, and mitigating both electronic and physical security incidents. The IT Director reviews and updates the Policy as needed for changes to the process.	Inspected the Incident Response Policy to verify a plan was in place to guide in identifying, responding to, and mitigating both electronic and physical security incidents. Inspected the Incident Response Policy version history to verify the IT Director reviewed and updated the Policy as needed for changes to the process.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	66 BCP - A Business Continuity Plan (BCP) is in place to help ensure timely resumption of critical business operations and systems in the event of various scenarios such as cyber attack, environmental event or similar disaster. The BCP is executed or tested at least annually and updated for lessons learned.	Inspected the Business Continuity Plan (BCP) to verify a plan was in place to help ensure timely resumption of critical business operations and systems in the event of various scenarios such as cyber attack, environmental event or similar disaster. Inspected the results of the BCP execution and plan updates to verify the BCP was executed or tested at least annually and updated for lessons learned.	No exceptions noted.
		67 An Incident Response Policy is in place to guide in identifying, responding to, and mitigating both electronic and physical security incidents. The IT Director reviews and updates the Policy as needed for changes to the process.	Inspected the Incident Response Policy to verify a plan was in place to guide in identifying, responding to, and mitigating both electronic and physical security incidents. Inspected the Incident Response Policy version history to verify the IT Director reviewed and updated the Policy as needed for changes to the process.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 7	**Common Criteria Related to System Operations**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		68 Subrogation and claims data backups for LSS systems and applications are performed on a scheduled basis. The completion of backups are monitored by the IT System Administrator for successful completion. Backup job failures are rerun the next business day.	Inspected the backup jobs, schedules and results of backups to verify subrogation and claims data backups for LSS systems and applications were performed on a scheduled basis. Inspected the backup alert notification configuration to verify the IT System Administrator monitored the completion of backups for successful completion. Inquired with IT management and inspected the backup log to verify there were no failed backups during the period.	No exceptions noted on the backup job schedules and monitoring. Unable to test the operating effectiveness of backup job failure reruns because there were no failed backups during the period.
		69 The SubroChain® claim file storage system is replicated to a second data center, providing redundancy and geographical dispersity.	Inspected the SubroChain® claim file storage replication settings to verify the SubroChain® claim file storage system was replicated to a second data center to provide for redundancy and geographical dispersity.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 8	**Common Criteria Related to Change Management**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**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.	96 SubroChain® and Client Access system changes are reviewed by IT management for completeness, discussed, and approved during weekly management meetings.	Inspected the change documentation for a sample of SubroChain® system changes to verify SubroChain® system changes were reviewed by IT management for completeness, discussed, and approved during weekly management meetings. Inquired with IT management and inspected the Client Access system log to verify there were no changes to the Client Access system during the period.	No exceptions noted on the SubroChain® system change reviews, discussions and approvals. Unable to test the operating effectiveness of the Client Access system changes because there were no changes during the period.
		102 SubroChain® and Client Access system changes are tested and then approved by management prior to deployment.	Inspected the change documentation for a sample of SubroChain® system changes to verify SubroChain® system changes were tested and then approved by management prior to deployment. Inquired with IT management and inspected the Client Access system log to verify there were no changes to the Client Access system during the period.	No exceptions noted with the SubroChain® system changes. Unable to test the operating effectiveness of the Client Access system changes because there were no changes during the period.
		103 The Change Management Policy sets standards that ensure consistent and expected results during enhancements, implementations or other system changes.	Inspected the Change Management Policy to verify the Policy set standards that ensured consistent and expected results during enhancements, implementations or other system changes.	No exceptions noted.
		104 Changes to in-scope systems are logged and tracked in a ticketing system to ensure changes flow through the appropriate change management steps.	Inspected the log of system changes from the in-scope ticketing systems to verify system changes were logged and tracked to ensure changes flowed through the appropriate change management steps.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 8	**Common Criteria Related to Change Management**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		105 Security patches on Latitude-controlled endpoints and servers are applied monthly or as needed based on criticality to enhance performance and protect systems from vulnerabilities.	Inspected examples of security patches applied to Latitude-controlled endpoints and servers to verify security patches were applied monthly or as needed based on criticality to enhance performance and protect systems from vulnerabilities.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 9	**Common Criteria Related to Risk Mitigation**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	66 BCP - A Business Continuity Plan (BCP) is in place to help ensure timely resumption of critical business operations and systems in the event of various scenarios such as cyber attack, environmental event or similar disaster. The BCP is executed or tested at least annually and updated for lessons learned.	Inspected the Business Continuity Plan (BCP) to verify a plan was in place to help ensure timely resumption of critical business operations and systems in the event of various scenarios such as cyber attack, environmental event or similar disaster. Inspected the results of the BCP execution and plan updates to verify the BCP was executed or tested at least annually and updated for lessons learned.	No exceptions noted.
		67 An Incident Response Policy is in place to guide in identifying, responding to, and mitigating both electronic and physical security incidents. The IT Director reviews and updates the Policy as needed for changes to the process.	Inspected the Incident Response Policy to verify a plan was in place to guide in identifying, responding to, and mitigating both electronic and physical security incidents. Inspected the Incident Response Policy version history to verify the IT Director reviewed and updated the Policy as needed for changes to the process.	No exceptions noted.
		68 Subrogation and claims data backups for LSS systems and applications are performed on a scheduled basis. The completion of backups is monitored by the IT System Administrator for successful completion. Backup job failures are rerun the next business day.	Inspected the backup jobs, schedules and results of backups to verify subrogation and claims data backups for LSS systems and applications were performed on a scheduled basis. Inspected the backup alert notification configuration to verify the IT System Administrator monitored the completion of backups for successful completion. Inquired with IT management and inspected the backup log to verify there were no failed backups during the period.	No exceptions noted on the backup job schedules and monitoring. Unable to test the operating effectiveness of backup job failure reruns because there were no failed backups during the period.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 9	**Common Criteria Related to Risk Mitigation**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		69 The SubroChain® claim file storage system is replicated to a second data center, providing redundancy and geographical dispersity.	Inspected the SubroChain® claim file storage replication settings to verify the SubroChain® claim file storage system was replicated to a second data center to provide for redundancy and geographical dispersity.	No exceptions noted.
		35 Insurance - Latitude retains corporate insurance to provide risk transfer for major exposures such as cyber and business risk.	Inspected the Latitude insurance policies to verify the Company retained corporate insurance to provide risk transfer for major exposures such as cyber and business risk.	No exceptions noted.
		109 Production data for Latitude-controlled systems is restored periodically to ensure data can be successfully recovered if needed.	Inspected examples of production data restores to verify production data for Latitude-controlled systems was periodically restored to ensure data could be successfully recovered if needed.	No exceptions noted.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	38 Attorney Firm Insurance - The Legal department, who coordinates the use of attorney law firm vendors who handle subrogation litigation on behalf of Latitude for its clients, ensures that each firm maintains professional liability insurance annually.	Inspected the tracking spreadsheet of attorney law firm vendors who handle subrogation litigation on behalf of Latitude to verify the Legal department ensured each firm maintained professional liability insurance annually.	No exceptions noted.
		97 Annually, the IT Director reviews attestation reports for its SaaS and IaaS service providers to evaluate the effectiveness of controls critical to the operation of LSS's SubroChain® system. Deficiencies are reported and discussed in monthly SubroChain Steering Committee meetings to determine corrective course of action as needed.	Inspected the attestation report review presentations to verify the IT Director reviewed attestation reports for its SaaS and IaaS service providers, evaluated the effectiveness of controls critical to the operation of LSS's SubroChain® system, and reported and discussed deficiencies during the SubroChain Steering Committee meeting to determine any necessary corrective courses of action.	No exceptions noted.

AVAILABILITY CRITERIA				
A	**Additional Criteria for Availability**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**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.	106 IT management is notified when capacity issues for cloud-based, Latitude-controlled systems are detected. Additional capacity can be increased on demand as needed.	Inspected an example of a capacity notification and adjustment to verify IT management was notified when capacity issues for cloud-based, Latitude-controlled systems were detected and additional capacity could be increased on demand as needed.	No exceptions noted.
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.	68 Subrogation and claims data backups for LSS systems and applications are performed on a scheduled basis. The completion of backups are monitored by the IT System Administrator for successful completion. Backup job failures are rerun the next business day.	Inspected the backup jobs, schedules and results of backups to verify subrogation and claims data backups for LSS systems and applications were performed on a scheduled basis. Inspected the backup alert notification configuration to verify the IT System Administrator monitored the completion of backups for successful completion. Inquired with IT management and inspected the backup log to verify there were no failed backups during the period.	No exceptions noted on the backup job schedules and monitoring. Unable to test the operating effectiveness of backup job failure reruns because there were no failed backups during the period.
		69 The SubroChain® claim file storage system is replicated to a second data center, providing redundancy and geographical dispersity.	Inspected the SubroChain® claim file storage replication settings to verify the SubroChain® claim file storage system was replicated to a second data center to provide for redundancy and geographical dispersity.	No exceptions noted.

AVAILABILITY CRITERIA				
A	**Additional Criteria for Availability**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		108 Latitude's computer room is electronically monitored for temperature and humidity to protect the network equipment. Management is notified when temperature and humidity exceed pre-defined tolerance levels.	Inspected the environmental monitoring setting to verify Latitude's computer room was electronically monitored for temperature and humidity to protect the network equipment. Inspected the monitoring alert setting to verify thresholds were established and management was notified when temperature and humidity exceeded pre-defined tolerance levels.	No exceptions noted.
		109 Production data for Latitude-controlled systems is restored periodically to ensure data can be successfully recovered if needed.	Inspected examples of production data restores to verify production data for Latitude-controlled systems was periodically restored to ensure data could be successfully recovered if needed.	No exceptions noted.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	66 BCP - A Business Continuity Plan (BCP) is in place to help ensure timely resumption of critical business operations and systems in the event of various scenarios such as cyber attack, environmental event or similar disaster. The BCP is executed or tested at least annually and updated for lessons learned.	Inspected the Business Continuity Plan (BCP) to verify a plan was in place to help ensure timely resumption of critical business operations and systems in the event of various scenarios such as cyber attack, environmental event or similar disaster. Inspected the results of the BCP execution and plan updates to verify the BCP was executed or tested at least annually and updated for lessons learned.	No exceptions noted.
		109 Production data for Latitude-controlled systems is restored periodically to ensure data can be successfully recovered if needed.	Inspected examples of production data restores to verify production data for Latitude-controlled systems was periodically restored to ensure data could be successfully recovered if needed.	No exceptions noted.

Section 5:

Other Information Provided by Latitude That Is Not Covered by the Service Auditor's Report

MANAGEMENT'S RESPONSE TO EXCEPTIONS

In addition to the information in Section 3, "Latitude's Description of Its Subrogation and Salvage Recovery Services and Vehicle Material Damage Appraisal Services System," and the controls outlined in Section 4, "Control Objectives, Related Controls and Tests of Controls," the following additional information is being provided as it may be relevant to the reader to obtain a better understanding of Latitude's exceptions and subrogation and salvage recovery services and vehicle material damage appraisal services. The following Management's Response to the exceptions noted in Section 4 and disclosures regarding processes and controls are not within the scope of this examination and have not been audited.

Control Activity	Test Results	Management's Response
CO 1 Organization and Administration Controls – Controls provide reasonable assurance that Corporate personnel are properly vetted, understand their responsibilities within their reporting structure and adhere to company policies and procedures.		
5 *Performance Evaluations* - Employee performance reviews are conducted within the new employee's probationary period and annually thereafter to ensure satisfactory performance, conduct and compliance with company requirements and standards.	Exceptions noted on the employee annual performance reviews. For 1 of 3 (33.3%) IC employees, completion of the performance review was not tracked.	Latitude's HR department began tracking the completion of InspectionConnection employee performance reviews in October 2022. This action was part of the gradual integration of InspectionConnection practices following their acquisition on July 15, 2021. We believe the procedures in effect since October 2022 are effective.

Control Activity	Test Results	Management's Response
CO 12 – Logical Access: Controls provide reasonable assurance that logical access to key information systems is managed and limited to authorized users.		
73 A role-based access control (RBAC) matrix, security groups and an Employee Onboarding Checklist are utilized to set up new employee access to LSS systems and applications. Access to systems and assigned permissions are based on the principle of least privileges. Additional access or access changes are approved by the user's supervisors prior to access being provisioned.	Exceptions noted on SubroChain® access change documentation. The SubroChain® listing of user access changes between April 1, 2022 - December 31, 2022 was not available due to system limitations.	We are investigating options to increase our logging of user additions, deletions, and changes to ensure future user system RBAC, onboarding, and offboarding audits can be completed. SubroChain® (Salesforce) does indeed store access changes through the included logging feature – which were successfully used during this audit. Proof of all user access changes that were requested by management in an IT service ticket was successfully provided during this audit. No requested access changes were found to be unfulfilled as recorded in system logs. A user access change report has not been created in SubroChain because the requests are rare (1-3 per year) and handled by IT service tickets until the employee has the required access as requested by their manager to perform their job.

Control Activity	Test Results	Management's Response
CO 11 – Physical Access: Controls provide reasonable assurance that physical access to information, key computing resources and sensitive areas is adequately controlled and limited to authorized personnel.		
75 HR completes an Employee Departure Checklist to ensure requests for removal of system access and physical access to the Latitude Corporate Office is not overlooked. Once notified, IT disables access in a timely manner.	Exceptions noted on the physical access removals for LSS terminated employees. For 2 of 2 (100%) LSS terminated employees with physical access to the corporate office, documentation showing HR completed an Employee Departure Checklist and IT removed physical access could not be provided.	An annual audit conducted by LSS IT ensures that all terminated employees do not have access to any physical or logical systems. IT personnel use the Employee Departure Checklist as a guide to ensure physical and logical access is removed for terminated employees. We have confirmed that there have not been any incidents of terminated employees having access to or accessing the physical office to date due to our office being equipped with multiple layers of installed physical security. All office access is recorded on biometric door readers, security cameras, and an active alarm system protecting all points of entry. Both the security camera and alarm systems are monitored 24/7 by LSS management and a professional monitoring service, which Latitude purchased all available options.