armanino

System and Organization Controls (SOC) 2

Type 2 Report on Controls Relevant to the Security Trust Services Category

April 1, 2024 to July 31, 2024

REPORT PREPARED FOR

Centerbase

TABLE OF CONTENTS

INDEPENDENT SERVICE AUDITOR'S REPORT

To the Management of

Centerbase, LLC

Dallas, Texas

Scope

We have examined Centerbase, LLC's ("Centerbase", "Centerbase, LegalFit, and Family Law Software", or the "Company") accompanying description of its law firm management suite found in Section III titled "Description of the System" throughout the period April 1, 2024 to July 31, 2024 (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)* (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, 2024 to July 31, 2024, to provide reasonable assurance that Centerbase's service commitments and system requirements were achieved based on the trust services criteria relevant to security (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)* (AICPA, *Trust Services Criteria*).

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

Centerbase uses subservice organizations, Amazon Web Services ("AWS") and TierPoint, LLC ("TierPoint"), to provide cloud infrastructure services and colocation services, respectively. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Centerbase, to achieve Centerbase's service commitments and system requirements based on the applicable trust services criteria. The description presents Centerbase's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Centerbase's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The information included in Section V, "Other Information Provided by Management Not Covered by the Service Auditor's Report," is presented by Centerbase's management to provide additional information and is not part of Centerbase's description of its law firm management suite made available to user entities during the period April 1, 2024 to July 31, 2024. Information about Centerbase's response to the noted exceptions has not been subjected to the procedures applied in the examination and accordingly, we express no opinion on it.

Service Organization's Responsibilities

Centerbase 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 Centerbase's service commitments and system requirements were achieved.

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

Service Auditor's Responsibilities

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

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

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

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs. There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design or operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

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

Service Auditor's Independence

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

Opinion

In our opinion, in all material respects—

a. The description presents Centerbase's law firm management suite that was designed and implemented throughout the period April 1, 2024 to July 31, 2024, in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period April 1, 2024 to July 31, 2024, to provide reasonable assurance that Centerbase's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organizations and user entities applied the complementary controls assumed in the design of Centerbase's controls throughout that period.

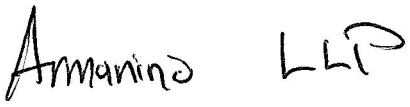
c. The controls stated in the description operated effectively throughout the period April 1, 2024 to July 31, 2024, to provide reasonable assurance that Centerbase's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Centerbase's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of Centerbase; user entities of Centerbase's law firm management suite during some or all of the period April 1, 2024 to July 31, 2024, business partners of Centerbase subject to risks arising from interactions with the system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

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



Armanino LLP

San Ramon, California

October 22, 2024

MANAGEMENT'S ASSERTION

We have prepared the accompanying description of Centerbase, LLC's ("Centerbase", "Centerbase, LegalFit, and Family Law Software", or the "Company") law firm management suite titled "Description of the System" throughout the period April 1, 2024 to July 31, 2024 (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)* (AICPA, *Description Criteria*), (description criteria). The description is intended to provide report users with information about the system that may be useful when assessing the risks arising from interactions with Centerbase's system, particularly information about system controls that Centerbase 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 (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)* (AICPA, *Trust Services Criteria*).

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Centerbase, to achieve Centerbase'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.

Centerbase uses subservice organizations, Amazon Web Services ("AWS") and TierPoint, LLC ("TierPoint"), to provide cloud infrastructure services and colocation services, respectively. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Centerbase, to achieve Centerbase's service commitments and system requirements based on the applicable trust services criteria. The description presents Centerbase's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Centerbase's controls. The description does not disclose the actual controls at the subservice organizations.

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

1) The description presents Centerbase's law firm management suite that was designed and implemented throughout the period April 1, 2024 to July 31, 2024, in accordance with the description criteria.
2) The controls stated in the description were suitably designed throughout the period April 1, 2024 to July 31, 2024, to provide reasonable assurance that Centerbase's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations and user entities applied the complementary controls assumed in the design of Centerbase's controls throughout that period.
3) The controls stated in the description operated effectively throughout the period April 1, 2024 to July 31, 2024, to provide reasonable assurance that Centerbase'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 Centerbase's controls operated effectively throughout that period.

DESCRIPTION OF THE CENTERBASE LAW FIRM MANAGEMENT SUITE

Overview of Operations

Company Overview

Founded in 2014, Centerbase, LLC ("Centerbase" or the "Company") delivers a customizable, cloud-based legal practice management solution which gives small to mid-sized law firms the power to streamline their daily tasks with ease and efficiency. Centerbase acquired Family Law Software (FLS) and LegalFit (LF) in 2021. Centerbase delivers the power of legacy systems with the flexibility of the cloud to modernize its law firm client-base without sacrificing functionality. The Company is a full service, customer-centric organization dedicated to creating value and delivering results.

Services Provided

The current product offerings allow customers to:

- Centerbase – Allows users to leverage an all-in-one management solution combining day to day workflow, matter management, document management, time, billing, and accounting.
- LegalFit – Allows users to create and manage their law firm's website, as well as perform general marketing tasks.
- Family Law Software – Allows users to complete financial analysis and support calculations relative to family law cases.

In-scope Applications

The SOC 2 report includes testing of the following in-scope applications:

Application	Description
Centerbase	Centerbase is a cloud-based legal practice management solution that combines workflow, matter management, document management, time and billing, and accounting into a single platform.
LegalFit	Centerbase LegalFit is a cloud-based website content management system and marketing platform for law firms.
Family Law Software	Centerbase Family Law Software is a cloud-based platform that allows its users to easily and accurately complete financial analysis and support calculations for fast family law case resolution.

Principal Service Commitments and System Requirements

Key commitments:

- Securing customer data
- Maintaining 24/7 system availability
- Classifying data and maintaining confidentiality of data classified as such

Examples of system requirements to achieve the above commitments include:

- Logical and physical access controls over customer data
- Redundant systems that would ensure 24/7 availability
- Authority of classifying data is assigned to a specific individual or group
- Confidential data is segregated in a location that can be accessed only by authorized individuals

Significant Changes to the System

There were no changes that are likely to affect report users' understanding of how the systems are used to provide the services for the period April 1, 2024 to July 31, 2024.

RELEVANT ASPECTS OF INTERNAL CONTROL

As defined by the American Institute of Certified Public Accountants (AICPA), internal control is a process affected by an entity's board of directors, management, and other personnel and consists of five interrelated components:

- Control Environment
- Risk Management
- Information and Communication
- Monitoring
- Control Activities

This section briefly describes the essential characteristics and other interrelated components over the trust services criteria of security as they pertain to the Company.

Control Environment

Management and the board of directors take their role in overseeing internal controls seriously. The Company has a code of conduct and a procedure for reporting violations. This information is posted on the Company intranet. The Company distributes the code of conduct as part of the employee manual to all new employees and requires each employee to acknowledge that they have read and understand the code of conduct. The Company believes it has the proper incentives in place that would tend to discourage conflicts of interest and/or improper behavior. Company exercises significant diligence in hiring competent, qualified professionals, and to then provide employees with the appropriate on-the-job training. Company employees receive safety training, new hire orientation training, and most employees receive continuing education through online industry-related trainings and periodic industry conferences. The board of directors has sufficient independence to effectively oversee management.

The Company management team meets at least monthly. The members of the management team are the:

- Chief Executive Officer
- Chief Financial Officer
- Chief People Officer
- Chief Technology Officer
- Chief Marketing Officer
- Vice President, Customer Operations
- General Manager, Mid Law
- General Manager, Small Law

Control Environment (continued)

The Centerbase strategic plan, which is captured in the Centerbase mission statement, was enacted by the CEO with contributions from the entire management team. The strategic plan focuses on corporate strategy for developing the core business, improving current product offerings, expanding solutions, and responding to market challenges. Annually, management reviews and develops plans and resources to meet strategic goals. Relevant segments of the strategic plan are shared with members of the management team, who disseminate the strategic goals to personnel, and monitor progress and adherence to the strategic plan.

Centerbase has a defined organizational structure. The Company organizational chart is made available to all employees, and reporting relationships are kept current on that chart. Roles and responsibilities are defined in written job descriptions and communicated to employees, as well as supervisors and managers. Senior management periodically reviews reporting relationships and the organizational structure as part of planning and adjusts the reporting structures, as needed, based on changing commitments, requirements and goals.

Human Resources

The Centerbase Chief People Officer, as well as upper management, oversee other human resources (HR) functions, including employee search, recruiting, orientation and industry-related training.

The Centerbase HR function is guided by established policies and procedures for hiring, promoting and compensating, training, and termination of employees. Relevant Centerbase policies and procedures are outlined in the Centerbase employee handbook provided to all employees. Centerbase policies include probation, suspension or termination as potential sanctions for employee misconduct. Employees are required to respond in writing with an acknowledgement of receipt and understanding of the Centerbase employee handbook.

Polices included in the employee handbook include, but are not limited to:

- Code of conduct,
- Benefit information,
- General office information,
- Job classification status,
- Anti-harassment,
- Equal employment opportunity,
- Electronic communication policies
- Confidential information, and
- Prohibited conduct

Employee compliance with behavioral expectations is evaluated as part of their job performance. Candidates for promotion must have demonstrated a commitment to ethical standards through their own actions, and by setting an example for other employees.

Information is accumulated primarily through the performance evaluation process, and less formally through emails or comments submitted by supervisors or peers. Complaints indicating departure from behavioral standards are investigated by managers and are documented, as necessary.

As part of Centerbase's performance management process, all managers are required to establish expectations and evaluate performance for the employees they manage. Quarterly, managers meet with their employees on an individual basis to discuss performance over the past three months and set expectations for the coming three months. These evaluations are facilitated through management meetings where results of employee performance are discussed. Performance is documented Motivosity.

Control Environment (continued)

Human Resources (continued)

A critical part of providing a work environment with strong ethics and controls starts with the hiring and training processes. Management takes an active role in recruitment, including screening applicants, checking references, completing background checks, administering drug testing, and providing the orientation of new team members.

Potential employees must undergo a criminal background check and drug screening before beginning work at Centerbase.

New Hire Onboarding

Before an individual joins the Centerbase team, management must first identify the need for additional personnel. A job requisition is drafted and approved by the CEO. If the job requisition does not have a corresponding job description, one is created and reviewed by the appropriate manager. Once the requisition has been completed, a job description is drafted. This is then posted internally and to various online job boards and career sites.

The Centerbase management team reviews resumes to identify qualified candidates. When a qualified candidate is identified he or she is further evaluated through a phone screening process. If the candidate passes the phone screening they are scheduled for in person interview with the individuals in the respective team in which they will work.

When interviews are completed, a hiring decision is made. If management chooses to issue an offer letter to the prospective hire, Centerbase management contacts the HR team, who assists with issuance of the offer letter and communication with prospective employee. If the prospective employee formally accepts the offer letter, HR team completes a background check and drug screening for the individual. The formal background check and hiring steps must be complete before the prospective Centerbase employee is allowed access to Centerbase premises to begin work.

When the new employee arrives on his or her first day, they meet with the Centerbase HR Generalist to review necessary paperwork. They are required to provide written acknowledgement of the Centerbase employee handbook. The new employee then attends a new employee orientation (NEO) seminar. After orientation is complete, the individual is escorted to their work area where training continues through on the job training.

Throughout the hiring process, progress and completion of tasks are recorded on a new hire checklist. This checklist is maintained by the Centerbase people team and is included in the employee's file.

Policy for Training

All new employees are required to attend NEO that introduces them to the Centerbase culture, business operations, policies and procedures, and the applications comprising the Centerbase system.

Ongoing employee training consists principally of on-the-job training. When external training for an employee will contribute to Centerbase's business goals, Centerbase will pay for pre-approved, job-related courses and related travel expenses. Additionally, Centerbase offers optional internal training seminars regarding specific Centerbase products and processes. Employees are also provided access to industry publications and resources for continued self-education in their respective professional field, legal tech industry trends, regulatory requirements, etc. The Centerbase people team monitors compliance with corporate-wide training requirements (Jobsite safety, sexual harassment, etc.).

Control Environment (continued)

Code of Conduct

The Centerbase employee manual, which contains the code of conduct is available to all employees on Centerbase's intranet and includes sections that address business conduct, conflicts of interest, financial reporting, safeguarding of company assets and other information related to corporate conduct and culture. This document makes Centerbase's position clear that violations of the code of conduct will not be tolerated and will lead to disciplinary action, including possible termination.

Employment Termination

Employment can be terminated by Centerbase at any time as it operates as an at-will employer. Employee terminations can be voluntary or involuntary. Involuntary terminations require prior documentation of issues and performance coaching with the individual to resolve those issues.

Risk Assessment

As part of Centerbase's risk management activities, Centerbase conducts an annual enterprise risk assessment. The assessment is a collaborative, face-to-face whereby the management team draws on collective industry, enterprise, technical, and regulatory knowledge to identify key risks to business operations. As part of the management team meeting, a formal risk assessment report is created to memorialize identified risks, risk rankings and mitigation strategies. The Risk Assessment Report guides internal risk management and monitoring activities for the forthcoming year. The Risk Assessment Report is revisited and revised for marked changes or developments in market, industry, regulatory or legal risks.

As part of the annual risk assessment and formal Risk Assessment Report, management identifies information technology risks, ranks those risks, and develops mitigation strategies which are monitored by the Director of IT for successful mitigation. In addition to the annual risk assessment, risk is evaluated daily through defined and repeatable Information Technology and business processes. These processes consider a multitude of risks, including security, logical access, availability of application services, and confidentiality of customer data at the heart of the Centerbase system. Mitigations strategies are developed by management iteratively to respond in a nimble fashion to ever-changing risk landscapes.

The need for high availability warranted Centerbase's investment in redundant on premises and cloud infrastructure to support the Company's suite of applications, thereby reducing or eliminating single points of failure.

To support Information Technology risk management activities, management conducts annual penetration testing. Each item identified on the penetration tests is reviewed and prioritized for mitigation. Mitigations may include a change in policy as well as monitoring or periodic evaluation. Controls may be evaluated daily, weekly, monthly, or quarterly, per the risks and business needs.

Information and Communication

Information Systems

Centerbase's information systems have been engineered on the principles of high availability, security and confidentiality. To assist in achieving the desired level of consistency of these principles, Centerbase has located its American production environment within the city of Dallas, TX at TierPoint, Centerbase's Canadian production environment within CA Central (Qeubec) region of the Amazon Web Services (AWS) Elastic Compute Cloud (EC2), FLS has located its production environment within the US East (Ohio) region of the Amazon Web Services (AWS) Elastic Compute Cloud (EC2), and LegalFit has located its production environment within the US West (Oregon) region of the Amazon Web Services (AWS) Elastic Compute Cloud (EC2).

Information and Communication (continued)

Information Systems (continued)

The Centerbase application runs on servers which participate in an active Disaster Recovery Protocol. These systems are physically and logically secured from other components of the Centerbase corporate infrastructure.

Through methodology which is documented and tested within the Centerbase business continuity and disaster recovery plan, a portion of Centerbase's critical information systems are backed up via Veeam while being stored at the TierPoint colocation facility in Chicago. This increases system availability in the event of a disaster within the DFW Metroplex. FLS critical information systems are replicated to the Amazon Simple Storage Service (S3). This increases system availability in the event of a disaster within the AWS US East (Ohio) region as FLS can fail over to a set of replicated backup servers located in the AWS US West (Oregon) region. LF critical information systems are replicated to the Amazon Simple Storage Service (S3). This increases system availability in the event of a disaster within the AWS US West 2 (Oregon) region as LF can fail over to a set of replicated backup servers located in the AWS US West 2b (Oregon) availability zone.

Communication

Centerbase endeavors to inform internal and external users of the structure of the system so they may understand their role in the system and the results of system operation.

System descriptions are available to authorized external users that describe relevant system components as well as the purpose and design of the system.

Internal users learn about Centerbase systems beginning with their orientation and continuing as needed with on-the-job training and/or specific training courses. The corporate intranet holds both written documentation as well as links to specific training and policy documents on the Centerbase internal file server for Centerbase employees such as product and system information.

Centerbase typically conducts quarterly all-hands meetings. Traveling employees normally working outside of the corporate office attend the meeting via web or phone conference. The meeting is led by the Chief People Officer who along with the management team discusses the status of products and projects and any unusual items or events. The meetings also include an employee Q&A session to address specific concerns. These meetings allow senior management to communicate with employees about the strategy, results and values of the Company.

During business development presentations, the business development team provides documentation to prospective clients that describes the relationship between Centerbase and the client. As the business development team moves forward in the sales process, they review the standard contract terms and conditions with the prospective client to ensure a clear understanding of the anticipated roles of each party, including those related to system security commitments.

Some clients may request deviations from the standard terms of the Centerbase master services agreement (MSA). Deviations must be approved by designated executive management personnel. The executive management personnel evaluate all such deviations for their potential impact on Centerbase system security commitments.

The finalized MSA, service level agreement (SLA), SOW, and any other contract documents are stored within the Centerbase internal file server and access is restricted to personnel with a need to know.

Policies and procedures are a key tool for process standardization and communication of key control elements. Relevant policies and procedures are updated by their respective owners, with input and approval from the Director of IT and/or the designated compliance manager, and made available to Centerbase employees through the Centerbase internal file server. Changes in policies and procedures that impact internal users (employees) responsibilities regarding security commitments are communicated via email and in-person meetings.

Information and Communication (continued)

Communication (continued)

Monitoring systems assist Centerbase in meeting SLA requirements. Technical processes are monitored by automated systems such as DataDog and PRTG. Staff members receive automated alerts via Teams, a communication and messaging application, when there is a substantial decrease in system performance or a significant security event so they can respond to the issue.

Clients' responsibilities are defined in the MSA. Changes in contractual responsibilities relevant to security and/or other responsibilities are communicated to customers by management and memorialized in a new or amended MSA.

Monitoring

Monitoring activities are intended to identify and remediate areas of risk including strategic risk, financial risk, operational risk and legal/regulatory risk.

Management and supervisory personnel monitor the quality of internal control performance via frequent observation, interaction and performance of their assigned duties.

Critical job functions have been designed and implemented to provide inherent monitoring through separation of job functions, management oversight and systematic controls. Management reviews the functionality of software products and application configurations before they move through the development process and into production.

Logging and monitoring software platforms DataDog and PRTG are used to collect data from system infrastructure components and from endpoint systems. DataDog is configured for integration with AWS and monitors production data live through this integration. The logging and monitoring software is used to monitor system performance, potential security threats and vulnerabilities, and resource utilization, and to detect unusual system activity or service requests. This software sends an alert message via Teams to the appropriate team members. Further, Centerbase uses Drata to continuously monitor its information security controls.

Throughout each of the above processes, identified deficiencies are communicated to the relevant management personnel and appropriate follow up actions are initiated.

Use and Monitoring of Sub-Service Providers

Centerbase's Canadian production data center is in the CA Central (Quebec) region of the Amazon Web Services (AWS) Elastic Compute Cloud (EC2). The production data center hosts the Software as a Service ("SaaS") versions of the Centerbase product suite. Centerbase's American production data center resources are managed by internally leveraging VMWare and is hosted by the TierPoint colocation facility.

The Centerbase production data center is designed with fault tolerance protection for all layers of the platform and infrastructure, including network traffic and firewalls, as well as the web and application services and backend database connections. The Centerbase infrastructure is designed to scale substantially to accommodate foreseeable growth in the number of end-users and transaction volume for their products and services.

Centerbase monitors the performance of these activities with monitoring tools as described above. Issues or relevant exceptions are investigated further for impact to the Centerbase suite of applications.

The Centerbase production data center also replicates all critical production data to the disaster recovery site in Chicago. These replicated virtual machines are on standby and are ready to deploy in the event of a primary virtual server failure.

CONTROL ACTIVITIES

Policies and Procedures

Policies and procedures are a key tool for process standardization and communication of key control elements. Relevant policies and procedures are updated by their respective owners, reviewed at least annually, and made available to Centerbase employees through the Centerbase intranet. Information security policies include, but are not limited to:

- Information security policy
- Incident response plan
- Privacy policy
- Risk assessment policy
- Acceptable use policy
- Access control policy
- Physical security policy
- Data protection policy
- Asset management policy
- Software development life cycle

Security Awareness Training

Centerbase maintains a security awareness program through various mechanisms including:

- Employee orientation program,
- Annual security awareness training,
- Periodic email communications from the designated compliance manager and other management, and
- Role-specific security training

Access Provisioning

Employees are granted system access commensurate with their job responsibilities and based on the principle of least privilege. The departments' managers and IT management are responsible for assigning and maintaining access rights to the Centerbase internal and production network environments and related devices and applications.

For new hires, the people team files an onboarding ticket to the IT department requesting network and/or application access. The IT department reviews the request and validates that the request was provided by an authorized individual. Once IT management is satisfied that the request has been properly authorized, access is granted in accordance with the new hire checklist.

For changes to current user privileges, user access requests are approved by the employee's manager prior to being provisioned by IT management.

Access Deprovisioning

Account terminations are initiated by the people team via an employee offboarding ticket. Accounts are disabled or deleted by the IT department within one business day that the termination takes effect. This termination process includes:

- User access to all applications will typically be revoked or disabled within one business day that the termination takes effect.
- Access to the domain, administrator, database and critical network devices will typically be revoked or disabled in accordance with the information provided in the ticket.

CONTROL ACTIVITIES (continued)

Access Deprovisioning (continued)

- Physical assets such as equipment, and company credit cards (if applicable) are collected and noted on the ticket.

Under certain conditions, domain accounts may need to remain accessible after the termination date. In these cases, the account password is changed and the account is marked as locked. Any necessary data is migrated from the terminated account to an active account. When management determines that all necessary data has been preserved, the account is fully closed. Account termination requests are documented in the ticketing system. Completion dates are logged with each ticket. A termination process document listing the changes of access completed when terminating the employee is reviewed and signed by the terminated employee's department manager and IT management. This signed document is filed, which completes the overall termination process.

Physical Access

At least annually, Centerbse reviews the third-party audit reports for data center and colocation facility subservice providers to evaluate the design and operating effectiveness of physical access and environmental controls. Physical access to the Centerbase colocation facility is approved by an authorized individual prior to being granted. Physical access to the colocation facility is reviewed at least annually by management personnel.

Centerbase has security policies that have been approved by management and detail how physical access to the Company's headquarters is maintained.

Centerbase utilizes geographically separate locations to replicate production data across different regions.

Network Security Overview

All sensitive data transmitted and processed within the Centerbase network is encrypted to protect sensitive data against third-party disclosure in transit and customer data is encrypted at rest using strong encryption technologies. Servers and network components are secured with access control mechanisms and protected by hardened industry standard firewalls and intrusion detection systems. Further, disk encryption is enabled on all organization workstations. All security services are monitored and updated in a timely manner to address emerging vulnerabilities.

Centerbase has an established key management process in place to support the organization's use of cryptographic techniques. SSH production key users are limited to only designated personnel and users use unique accounts to access production machines. Users can only access the production system remotely through the use of encrypted communication systems. Centerbase leverages additional Amazon EC2 security capabilities for overall protection of its production environments.

Antivirus and Firewalls

Centerbase controls the introduction of software by restricting the ability to install software on workstations and laptops to user support personnel and to users with admin privileges over their own workstation or laptop.

Antivirus is installed on all workstations. Daily scans are scheduled for each machine. The antivirus software is configured to receive an updated virus signature at least daily. User support receives a report via email when any machine has not received an update in the required timeframe.

Centerbase utilizes several firewalls and AWS lines of defense to protect external points of connectivity and intrusion/extrusion detection systems to alert staff regarding unusual or unauthorized activity.

Network Security Overview (continued)

Antivirus and Firewalls (continued)

External access to sensitive data is restricted by user authentication and message encryption systems including TLS.

Intrusion Detection

Suspicious activity triggers alerts that are sent to responsible information security staff via Teams notifications. The responding individuals investigate the alerts and if necessary, escalate the issue following the defined incident response policy.

Vulnerability Assessment and Penetration Testing

The Centerbase production environment is monitored on an ongoing basis for known vulnerabilities. At least annually, Centerbase engages with a third-party vendor to perform penetration testing over the production environment. Additionally, on a quarterly basis, third party tools are used to perform vulnerability scans over the production environment.

Results of both the annual penetration testing and quarterly vulnerability scanning are reviewed by management, with high and critical priority findings being logged and tracked to resolution. Corrective action plans are defined as necessary with management oversight. The Company's risk assessment documentation is updated as necessary in part based on findings from the penetration testing and vulnerability scanning.

Administrator Access

Two-factor authentication is enforced for user accounts with access to sensitive systems and applications; this includes administrator access to the production platform.

A root account (also called an admin account or super-user account) is an account that is used to perform high-level tasks. Root accounts are common in all technology domains and acceptable in the corporate computing environment.

Root account privileges within Centerbase core systems are designated by IT management on an individual basis and not allowed unless in case of emergency.

Access Reviews

User access lists for applications, secured folders, root accounts and databases are reviewed by the Information security team leads at least annually. If any unnecessary access accounts (orphans) are found, appropriate remediation action is taken.

System Passwords

Users are required to enter a user ID and password to access any Centerbase network or application. Complexity standards for passwords have been established to enforce control. The following password policy settings are in place as system-based preventive controls for Active Directory and application accounts:

- Minimum length of 12 characters
- Maximum age 90 days
- Minimum age 30 days
- Account lockout after five (5) failed login attempts, locked accounts can only be reactivated by the Information Security team after authenticating the user
- Password history of five (5) passwords
- Passwords must meet complexity requirements.

Network Security Overview (continued)

Device Build and Hardening

New AWS EC2 instances are periodically deployed to the Centerbase network environment to support growth and management of the existing environment. Before an EC2 instance can be deployed, it must be assigned to the appropriate AWS network ACL(s) and security group(s). Additionally, Centerbase leverages server and database template clones for new deployments within its VMWare-managed environment.

System and Performance Monitoring

Centerbase leverages various tools and techniques to proactively monitor the production environment. These tools are designed to identify issues and alert responsible staff of the issue before it impacts Centerbase end users or customers. Tools that are currently leveraged include:

Tool	Description
DataDog	DataDog is a monitoring tool that provides monitoring over the performance and health of the Company's production environment.
PRTG	PRTG is a network monitoring tool that provides monitoring over usage and uptime of the production environment as well as server statistics.
AWS WAF	AWS WAF is a web application firewall that helps protect web applications from attacks by allowing configuration rules that allow, block, or monitor web requests based on pre-defined oversight conditions.
AWS GuardDuty	AWS GuardDuty monitors the production environment for malicious activity and delivers detailed security findings to designated personnel.
SonicWall	SonicWall is firewall that helps protect web applications from attacks by allowing configuration rules that allow, block, or monitor web requests based on pre-defined oversight conditions. SonicWall also functions as an IDS which monitors network traffic, identifies potential threats, and alerts designated personnel for a series of pre-defined alerts.

Security & Incident Management

Operations personnel follow defined protocols for evaluating and reporting events. Security related events are reported to the information technology department for evaluation and signed off by IT management. Centerbase provides a process to both employees and external users for reporting security incidents. Security incidents are tracked and prioritized according to severity.

If a security event is determined to be an incident, IT management directs the incident response team in following defined protocols for responding to the incident. These protocols are contained in the incident response policy manual. Root cause analyses are performed on critical incidents in order to provide IT management with heightened insight into the cause of the incident and for plans to prevent similar incidents from occurring. Resolution of security events are reviewed periodically at incident response team meetings. Changes in protocol or systems to improve response are addressed in these meetings. Changes are documented and signed off by the network administrator.

Internal and external users are informed of incidents in a timely manner and they are advised of any measures to be taken on their part. Governing entities are notified as required.

Network Security Overview (continued)

Change Management Policy

A formal change management process exists that governs changes to the applications and supporting infrastructure. The process document is reviewed by IT management on an annual basis and updated as needed.

The Company maintains separate development / test and production environments of the law firm management suite.

Change procedures are documented in a ticketing system. Once development has been completed, appropriate testing is performed. Test results are documented in a change ticket.

Upon successful completion of testing procedures, approval is documented before implementation into the production environment. Access to promote changes to production is restricted to authorized personnel based on job responsibilities.

Centerbase uses a version control system to manage source code, documentation, release labeling, and other change management tasks.

On a quarterly basis, management performs a comparison of change deployments against the corresponding change approvals to ensure no changes circumvented the change approval process.

Data Backup

The Company maintains backups of the production version of the law firm management suite code. Backups of the databases supporting the law firm management suite are performed using an automated backup utility configured to perform backups according to an established schedule of daily differential and bi-weekly full backups. Backups are encrypted at rest. Additionally, AWS Backup is leveraged for AWS-hosted production data where data is backed up daily and configured to store via AWS S3 buckets. Annually, the Company restores a subset of files from backup, and the results are verified as successful.

Disaster Recovery

Planning for the business continuity of Centerbase in the aftermath of a disaster is an essential part of an organization risk management program. Preparation for, response to, and recovery from a disaster affecting the administrative functions of the Company require the cooperative efforts of many functional areas and supporting organizations.

Because the Centerbase infrastructure is cloud-hosted between AWS and the TierPoint colocation facility, a disaster event occurring at the Centerbase headquarters would not impact production systems. If there was a major disaster that destroyed or severely compromised the infrastructure within the AWS US-East (Ohio) and US West (Oregon) regions, or the TierPoint Dallas, TX region, Centerbase has a disaster recovery policy in place. This policy provides the instructions regarding the transfer of production infrastructure and applications to the Centerbase 'warm' site hosted in the US-West (Oregon) region within AWS and the Chicago, IL region within TierPoint. The detailed procedure for failing-over to the Centerbase Warm Sites are outlined in the Centerbase disaster recovery plan.

Complementary Subservice Organization Controls

Subservice Organization Controls

The Company utilizes subservice organizations to perform the functions described below to improve operating and administrative effectiveness. Third party personnel are not granted access to Company or User Entity data or the Company systems themselves. The examination by the Independent Service Auditor did not extend to the policies and procedures at these subservice organizations.

AWS provides data center hosting services and DDoS monitoring and mitigation services. The servers hosted in AWS consist of virtual servers. AWS also provides managed DNS services for internal systems, and short term and long-term data storage for managing the content. TierPoint provides colocation services. Data center and colocation facilities are ISO 27001:2013 certified and undergo periodic SOC 1 and SOC 2 Type 2 examinations. Certification status and the results of examination are reviewed periodically as part of Company's monitoring controls and the vendor management process. Formal documentation of third-party vendor assessments is preserved for compliance purposes.

The facilities used during the reporting period and the data center hosting services relied upon by Company are listed in Table 1 and Table 2, respectively.

Table 1- Subservice organizations used by Centerbase

Entity	Facility Location	Services Hosted
Amazon Web Services ("AWS")	US West (Oregon), US East-1 (N. Virginia), US-East-2 (Ohio), CA-Central-1b (Canada)	Cloud hosting and infrastructure services
TierPoint, LLC ("TierPoint")	Dallas, TX	Colocation facility services

Table 2- Service Categories

Criteria	Complementary Subservice Organization Controls
CC6.4	• AWS and TierPoint are responsible for restricting data center access to authorized personnel. • AWS and TierPoint are responsible for the 24x7 monitoring of data centers by closed circuit cameras and security personnel.
A1.2 CC7.2	• AWS and TierPoint are responsible for the installation of fire suppression and detection, and environmental monitoring systems at the data centers. • AWS and TierPoint are responsible for protecting data centers against a disruption in power supply to the processing environment by an uninterruptible power supply (UPS). • AWS and TierPoint are responsible for overseeing the regular maintenance of environmental protections at data centers.

Complementary User Entity Controls

Centerbase's controls related to the Centerbase law firm management suite cover only a portion of overall internal control for each user entity of Centerbase. It is not feasible for the trust service criteria related to the Centerbase law firm management suite to be achieved solely by Centerbase. Therefore, each user entity's internal controls should be evaluated in conjunction with Centerbase's controls and the related tests and results described in Section IV of this report, taking into account the related complementary user entity controls, where applicable. In order for user entities to rely on the controls reported on herein, each user entity must evaluate its own internal controls to determine whether the identified complementary user entity controls have been implemented and are operating effectively.

This section highlights those internal control responsibilities that the Company believes should be present at each user entity and has considered in developing the Company's controls described in this report. Furthermore, the following list of controls is intended to address only those controls surrounding the interface and communication between the user entity and the Company. Accordingly, this list does not purport to be, and is not, a complete listing of the controls that a user entity should maintain. User entities are responsible for:

- Ensuring that the service agreement or quote with the Company properly describes the services to be provided.
- Communicating service level issues as they arise, including requesting reports of uptime for production servers if this becomes an issue.
- Communicating changes to the Company's services as required.
- Providing written notification of changes to individuals authorized to instruct the Company's activities on behalf of the client.
- Reporting operational failures, incidents, system problems/concerns, and complaints to appropriate Company personnel as client support requests on a timely basis (including resolution thereof).
- Requesting changes to the Centerbase law firm management suite and communicating issues with these changes after they have been implemented.
- Managing access provided to client personnel to its versions of the Centerbase law firm management suite.
- Reviewing release notes for changes to the Centerbase law firm management suite and evaluating the impact of changes to client control environments

Section IV - Trust Services Category, Criteria, Related Controls, Tests, and Test Results

Tests of Operating Effectiveness

Armanino's tests of the operating effectiveness of controls included tests that were considered necessary to evaluate whether the controls were sufficient to provide reasonable, but not absolute, assurance that the trust services criteria were satisfied throughout the report period. In selecting our test procedures, we considered various factors including, but not limited to, the following:

- the nature of the control being tested and its frequency
- the types and completeness of available evidence
- the trust services criteria to be satisfied
- the degree to which the control relies on the effectiveness of other controls
- whether the control is manual or automated
- the expected efficiency and effectiveness of the test.

Our tests of controls included observations, inspections, reperformance, and inquiries of appropriate management, supervisory, and staff personnel seeking relevant information regarding the controls. Additionally, the following table clarifies certain terms used in this section to describe the nature of the tests performed.

Test	Description
Inquiry	Inquiry of appropriate personnel and corroboration with management
Observation	Observation of the application, performance, or existence of the control
Inspection	Inspection of documents and reports indicating performance of the control
Reperformance	Reperformance of the control

Tests of Design and Implementation

Since inquiry of each control and inspection of the related policies was performed throughout our testing, these test procedures are not specified for each individual control and it is understood they apply as needed to controls in the subsequent pages.

TRUST SERVICES CATEGORY, CRITERIA, RELATED CONTROLS, TESTS, AND TEST RESULTS

The following tests of design, implementation, and operating effectiveness were completed to determine if controls necessary to meet the applicable trust services categories and associated criteria have been achieved throughout the examination period. Applicable Trust Services Categories for which controls were evaluated are:

- ***Security*** - The system is protected against unauthorized access (both physical and logical)

No other Trust Services Categories are included in the scope of this report.

Section IV - Trust Services Category, Criteria, Related Controls, Tests, and Test Results

CC1.0 Common Criteria Related to Control Environment

Trust Services Criteria	Control Ref #	Centerbase's Control Description	Test Procedure	Test Result
CC1.1 - COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	CC1.1.1	Centerbase management has approved all policies that detail how customer data may be made accessible and should be handled. These policies are accessible to all employees and contractors.	Inspected the policies related to customer data to determine whether management had approved each policy. Inspected the Company intranet to determine whether policies related to how customer data is handled were made available to all employees and contractors.	No exceptions noted
	CC1.1.2	Centerbase's new hires are required to pass a background check as a condition of their employment.	Inspected the background checks for a selection of new hires to determine whether the check was completed prior to the hire date.	No exceptions noted
	CC1.1.3	Company policies are accessible to all employees and, as appropriate, third parties. Personnel are required to acknowledge the information security policy and other topic-specific policies based on their job duties during onboarding and annually thereafter.	Inspected the Company intranet to determine whether all policies were made available to all employees and contractors. Inspected policy acknowledgements for a selection of new hires to determine whether each new hire acknowledged the information security policy during onboarding. Inspected policy acknowledgements for a selection of existing employees to determine whether each employee acknowledged the information security policy on an annual basis.	Exceptions noted: For 2 of 3 new hires sampled, the information security policy was not acknowledged within 30 days of hire. For 10 of 12 existing employees sampled, annual re-acknowledgment of the information security had not been performed within the last 12 months.

Section IV - Trust Services Category, Criteria, Related Controls, Tests, and Test Results

CC1.0 Common Criteria Related to Control Environment

Trust Services Criteria	Control Ref #	Centerbase's Control Description	Test Procedure	Test Result
CC1.1 - COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	CC1.1.4	Centerbase requires its contractors to read and acknowledge the code of conduct, read and acknowledge the acceptable use policy, and pass a background check.	Inspected the code of conduct acknowledgements for a selection of new contractors to determine whether they acknowledge the code of conduct upon hire. Inspected the background checks for a selection of new contractors to determine whether the check was completed prior to the hire date.	No exceptions noted
	CC1.1.5	Centerbase has a formal code of conduct approved by management and accessible to all employees. All employees must acknowledge the code of conduct upon hire.	Inspected the code of conduct acknowledgements for a selection of new hires to determine whether they acknowledge the code of conduct upon hire. Inspected the code of conduct to determine whether it was approved by management and made available to all employees.	No exceptions noted
CC1.2 - COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	CC1.2.1	The Company's board of directors or a relevant subcommittee is briefed by senior management at least annually on the state of the Company's cybersecurity and privacy risk. The board provides feedback and direction to management as needed.	Inspected the board meeting minutes to determine whether the Company's board of directors or a relevant subcommittee was briefed by senior management at least annually on the state of the Company's cybersecurity and privacy risk, and if necessary, the broad provided feedback to the management group.	No exceptions noted

Section IV - Trust Services Category, Criteria, Related Controls, Tests, and Test Results

CC1.0 Common Criteria Related to Control Environment

Trust Services Criteria	Control Ref #	Centerbase's Control Description	Test Procedure	Test Result
CC1.2 - COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	CC1.2.2	The Company's board of directors meets at least annually and maintains formal meeting minutes. The board includes directors that are independent of the Company.	Inspected the board meeting minutes to determine whether the board met annually and maintained formal meeting minutes. Inspected the board meetings to determine whether the board members are independent of the Company.	No exceptions noted
CC1.3 - COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	CC1.3.1	Roles and responsibilities are defined in written job descriptions and communicated to relevant personnel.	Inspected the job descriptions for a selection of new hires to determine whether it included qualifications, such as requisite skills and experience.	No exceptions noted
	CC1.3.2	Reporting relationships and organizational structures are reviewed periodically by senior management as part of organizational planning and adjusted as needed based on changing entity commitments and requirements.	Inspected the organization chart to determine whether reporting relationships and organizational structures were reviewed periodically by senior management as part of organizational planning and adjusted as needed based on changing entity commitments and requirements.	No exceptions noted

Section IV - Trust Services Category, Criteria, Related Controls, Tests, and Test Results

CC1.0 Common Criteria Related to Control Environment

Trust Services Criteria	Control Ref #	Centerbase's Control Description	Test Procedure	Test Result
CC1.3 - COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	CC1.3.3	Centerbase reviews its organizational structure, reporting lines, authorities, and responsibilities in terms of information security on an annual basis.	Inspected the organizational chart to determine whether Centerbase reviewed its organizational structure, reporting lines, authorities, and responsibilities in terms of information security on an annual basis.	No exceptions noted
CC1.4 - COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	CC1.4.1	Centerbase's new hires are required to go through an official recruiting process during which their qualifications and experience are screened to ensure that they are competent and capable of fulfilling their responsibilities.	Inspected the candidate evaluations for a selection of new hires to determine whether each new hire completed the recruiting process prior to hire.	No exceptions noted

Section IV - Trust Services Category, Criteria, Related Controls, Tests, and Test Results

CC1.0 Common Criteria Related to Control Environment

Trust Services Criteria	Control Ref #	Centerbase's Control Description	Test Procedure	Test Result
CC1.4 - COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	CC1.4.2	Centerbase has established training programs for privacy and information security to help employees understand their obligations and responsibilities to comply with Centerbase's security policies and procedures, including the identification and reporting of incidents. All full-time employees are required to complete the training upon hire and annually thereafter.	Inspected the Company's training documentation to determine whether Centerbase had established training programs for privacy and information security to help employees understand their obligations and responsibilities to comply with Centerbase's security policies and procedures, including the identification and reporting of incidents. Inspected training documentation for a selection of new hires to determine whether each employee completed the security training upon hire. Inspected training documentation for a selection of existing employees to determine whether each employee completed the security training on an annual basis.	Exceptions noted: For 3 of 3 new hires sampled, security training was not completed within 30 days of hire. For 2 of 12 existing employees sampled, security training had not been completed within the last 12 months.
CC1.5 - COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	CC1.5.1	Centerbase evaluates the performance of all employees through a formal, annual performance evaluation.	Inspected the performance evaluations for a selection of existing employees to determine whether each employee had a performance evaluation completed on an annual basis.	Exception noted: For 1 of 12 existing employees sampled, a performance evaluation had not been performed within the last 12 months.
	CC1.3.1	All Centerbase positions have a detailed job description that lists qualifications, such as requisite skills and experience, which candidates must meet in order to be hired by Centerbase.	Inspected the job descriptions for a selection of new hires to determine whether it included qualifications, such as requisite skills and experience.	No exceptions noted

Section IV - Trust Services Category, Criteria, Related Controls, Tests, and Test Results

CC1.0 Common Criteria Related to Control Environment

Trust Services Criteria	Control Ref #	Centerbase's Control Description	Test Procedure	Test Result
CC1.5 - COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	CC1.4.1	Centerbase's new hires are required to go through an official recruiting process during which their qualifications and experience are screened to ensure that they are competent and capable of fulfilling their responsibilities.	Inspected the candidate evaluations for a selection of new hires to determine whether each new hire completed the recruiting process prior to hire.	No exceptions noted

Section IV - Trust Services Category, Criteria, Related Controls, Tests, and Test Results

CC2.0 Common Criteria Related to Communication and Information

Trust Services Criteria	Control Ref #	Centerbase's Control Description	Test Procedure	Test Result
CC2.1 - COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	CC2.1.1	Centerbase has a defined information security policy that covers policies and procedures to support the functioning of internal control.	Inspected the information security policy to determine whether it covered policies and procedures to support the functioning of internal control.	No exceptions noted
	CC2.1.2	Management reviews security policies on an annual basis.	Inspected the Company's security policies to determine whether management reviewed each policy on an annual basis.	No exceptions noted
	CC1.1.1	Centerbase Management has approved all policies that detail how customer data may be made accessible and should be handled. These policies are accessible to all employees and contractors.	Inspected the policies related to customer data to determine whether management had approved each policy. Inspected the Company intranet to determine whether policies related to how customer data is handled were made available to all employees and contractors.	No exceptions noted
CC2.2 - COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	CC2.2.1	Centerbase maintains an accurate architectural diagram to document system boundaries to support the functioning of internal control.	Inspected the architectural diagram to determine whether it documented system boundaries that support the functioning of internal control.	No exceptions noted

Section IV - Trust Services Category, Criteria, Related Controls, Tests, and Test Results

CC2.0 Common Criteria Related to Communication and Information

Trust Services Criteria	Control Ref #	Centerbase's Control Description	Test Procedure	Test Result
CC2.2 - COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	CC2.2.2	Centerbase provides a process to employees for reporting security, confidentiality, integrity, and availability features, incidents, and concerns, and other complaints to company management.	Inspected the Company's intranet to determine whether Centerbase provided a process to employees for reporting security, confidentiality, integrity, and availability features, incidents, and concerns, and other complaints to company management.	No exceptions noted
	CC1.4.2	Centerbase has established training programs for privacy and information security to help employees understand their obligations and responsibilities to comply with Centerbase's security policies and procedures, including the identification and reporting of incidents. All full-time employees are required to complete the training upon hire and annually thereafter.	Inspected the Company's training documentation to determine whether Centerbase had established training programs for privacy and information security to help employees understand their obligations and responsibilities to comply with Centerbase's security policies and procedures, including the identification and reporting of incidents. Inspected training documentation for a selection of new hires to determine whether each employee completed the security training upon hire. Inspected training documentation for a selection of existing employees to determine whether each employee completed the security training on an annual basis.	Exceptions noted: For 3 of 3 new hires sampled, security training was not completed within 30 days of hire. For 2 of 12 existing employees sampled, security training had not been completed within the last 12 months.

Section IV - Trust Services Category, Criteria, Related Controls, Tests, and Test Results

CC2.0 Common Criteria Related to Communication and Information

Trust Services Criteria	Control Ref #	Centerbase's Control Description	Test Procedure	Test Result
CC2.3 - COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	CC2.3.1	Centerbase provides a process to external users for reporting security, confidentiality, integrity, and availability failures, incidents, concerns, and other complaints.	Inspected the Company's external website to determine whether Centerbase provided a process to external users for reporting security, confidentiality, integrity, and availability failures, incidents, concerns, and other complaints.	No exceptions noted
	CC2.3.2	Centerbase's security commitments are communicated to external users, as appropriate.	Inspected the Company's external website to determine whether Centerbase's security commitments were communicated to external users, as appropriate.	No exceptions noted
	CC2.3.3	Centerbase communicates system changes to customers that may affect security.	Inspected the Company's external website to determine whether Centerbase communicated system changes to customers that may affect security, availability, processing integrity, or confidentiality.	No exceptions noted
	CC2.3.4	Centerbase maintains a terms of service that is available to all external users and internal employees, and the terms detail the Company's security and availability commitments regarding the systems. Client agreements or master service agreements are in place for when the terms of service may not apply.	Inspected the terms of service to determine whether it was made available to all external users and internal employees, and the terms detailed the Company's security and availability commitments regarding the systems. Inspected the master service agreements for a selection of new customers to determine whether the agreement was in place for when the Terms of Service may not apply.	No exceptions noted

Section IV - Trust Services Category, Criteria, Related Controls, Tests, and Test Results

CC3.0 Common Criteria Related to Risk Assessment

Trust Services Criteria	Control Ref #	Centerbase's Control Description	Test Procedure	Test Result
CC3.1 - COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	CC3.1.1	Centerbase has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the risk management policies and procedures to determine whether they specified risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	No exceptions noted
CC3.2 - COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	CC3.2.1	Centerbase's management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Inspected the risk assessment documentation to determine whether management prepared a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	No exceptions noted
	CC3.2.2	Centerbase conducts a risk assessment at least annually.	Inspected the risk assessment to determine whether it was completed by Centerbase on an annual basis.	No exceptions noted

CC3.0 Common Criteria Related to Risk Assessment

Trust Services Criteria	Control Ref #	Centerbase's Control Description	Test Procedure	Test Result
CC3.2 - COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	CC3.2.3	Centerbase engages with a third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management.	Inspected the vulnerability scans for a selection of quarters to determine whether the scan was completed on a quarterly basis.	No exceptions noted
			Inspected the IT management meeting documentation to determine whether results were reviewed by management.	No exceptions noted
	CC3.2.4	Centerbase engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.	Inspected the penetration test to determine whether it was completed on an annual basis. Inspected the penetration test review documentation to determine whether the penetration test was reviewed by management and high priority findings are tracked to resolution.	No exceptions noted
	CC3.1.1	Centerbase has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the risk management policies and procedures to determine whether they specified risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	No exceptions noted

Section IV - Trust Services Category, Criteria, Related Controls, Tests, and Test Results

CC3.0 Common Criteria Related to Risk Assessment

Trust Services Criteria	Control Ref #	Centerbase's Control Description	Test Procedure	Test Result
CC3.3 - COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	CC3.1.1	Centerbase has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the risk management policies and procedures to determine whether they specified risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	No exceptions noted
	CC3.2.1	Centerbase's management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Inspected the risk assessment documentation to determine whether management prepared a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	No exceptions noted
	CC3.2.2	Centerbase conducts a risk assessment at least annually.	Inspected the risk assessment to determine whether it was completed by Centerbase on an annual basis.	No exceptions noted
CC3.4 - COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	CC3.4.1	Centerbase conducts continuous monitoring of security controls using Drata, and addresses issues in a timely manner.	Inspected the Drata platform to determine whether Centerbase conducted continuous monitoring of security controls using Drata, and addressed issues in a timely manner.	No exceptions noted

Section IV - Trust Services Category, Criteria, Related Controls, Tests, and Test Results

CC3.0 Common Criteria Related to Risk Assessment

Trust Services Criteria	Control Ref #	Centerbase's Control Description	Test Procedure	Test Result
CC3.4 - COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	CC3.1.1	Centerbase has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the risk management policies and procedures to determine whether they specified risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	No exceptions noted
	CC3.2.2	Centerbase conducts a risk assessment at least annually.	Inspected the risk assessment to determine whether it was completed by Centerbase on an annual basis.	No exceptions noted

Section IV - Trust Services Category, Criteria, Related Controls, Tests, and Test Results

CC4.0 Common Criteria Related to Monitoring Activities

Trust Services Criteria	Control Ref #	Centerbase's Control Description	Test Procedure	Test Result
CC4.1 - COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	CC4.1.1	The security team communicates important information security events to company management in a timely manner.	Inquired of management to understand the process by which the security team communicates important security events to company management. Inspected the system generated listing of security events to determine no security events during the examination period.	Non-occurrence: Armanino is unable to opine on the operating effectiveness of the control as there were no security events during the examination period.
	CC3.2.2	Centerbase conducts a risk assessment at least annually.	Inspected the risk assessment to determine whether it was completed by Centerbase on an annual basis.	No exceptions noted
	CC3.2.4	Centerbase engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.	Inspected the penetration test to determine whether it was completed on an annual basis. Inspected the penetration test review documentation to determine whether the penetration test was reviewed by management and high priority findings are tracked to resolution.	No exceptions noted

Section IV - Trust Services Category, Criteria, Related Controls, Tests, and Test Results

CC4.0 Common Criteria Related to Monitoring Activities

Trust Services Criteria	Control Ref #	Centerbase's Control Description	Test Procedure	Test Result
CC4.2 - COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	CC3.1.1	Centerbase has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the risk management policies and procedures to determine whether they specified risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	No exceptions noted
	CC3.2.1	Centerbase's management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Inspected the risk assessment documentation to determine whether management prepared a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	No exceptions noted
	CC3.2.2	Centerbase conducts a risk assessment at least annually.	Inspected the risk assessment to determine whether it was completed by Centerbase on an annual basis.	No exceptions noted

Section IV - Trust Services Category, Criteria, Related Controls, Tests, and Test Results

CC5.0 Common Criteria Related to Control Activities

Trust Services Criteria	Control Ref #	Centerbase's Control Description	Test Procedure	Test Result
CC5.1 - COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	CC5.1.1	Centerbase ensures that virtual machine OS patches are applied quarterly.	Inspected the patch updates for a selection of quarters and databases to determine whether virtual machine OS patches were applied monthly.	Exception noted: For 1 of 10 virtual machines sampled, patching had not been performed for the quarter tested.
	CC5.1.2	Centerbase's workstations operating system (OS) security patches are applied automatically.	Inspected the mobile device management configuration to determine whether Centerbase's workstations operating system (OS) security patches were applied automatically.	No exceptions noted
	CC3.1.1	Centerbase has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the risk management policies and procedures to determine whether they specified risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	No exceptions noted
	CC3.2.1	Centerbase's management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Inspected the risk assessment documentation to determine whether management prepared a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	No exceptions noted
	CC3.2.2	Centerbase conducts a risk assessment at least annually.	Inspected the risk assessment to determine whether it was completed by Centerbase on an annual basis.	No exceptions noted

Section IV - Trust Services Category, Criteria, Related Controls, Tests, and Test Results

CC5.0 Common Criteria Related to Control Activities

Trust Services Criteria	Control Ref #	Centerbase's Control Description	Test Procedure	Test Result
CC5.2 - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	CC1.1.1	Centerbase management has approved all policies that detail how customer data may be made accessible and should be handled. These policies are accessible to all employees and contractors.	Inspected the policies related to customer data to determine whether management had approved each policy. Inspected the Company intranet to determine whether policies related to how customer data is handled were made available to all employees and contractors.	No exceptions noted
	CC3.2.2	Centerbase conducts a risk assessment at least annually.	Inspected the risk assessment to determine whether it was completed by Centerbase on an annual basis.	No exceptions noted
CC5.3 - COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	CC5.3.1	Centerbase has policies and procedures in place to establish acceptable use of information assets approved by management, posted on the Company wiki, and accessible to all employees. All employees must acknowledge the acceptable use policy upon hire.	Inspected the policies detailing acceptable use of information assets to determine whether they were approved by management, and posted on the Company wiki for employees to access. Inspected the policy acknowledgements for a selection of new hires to determine whether each employee acknowledged policy documents detailing acceptable use of information assets upon hire.	No exceptions noted
	CC5.3.2	Hardening standards are in place to ensure that newly deployed server instances are appropriately secured.	Inspected the hardening standards to determine whether they were in place to ensure that newly deployed server instances are appropriately secured.	No exceptions noted

Section IV - Trust Services Category, Criteria, Related Controls, Tests, and Test Results

CC5.0 Common Criteria Related to Control Activities

Trust Services Criteria	Control Ref #	Centerbase's Control Description	Test Procedure	Test Result
CC5.3 - COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	CC2.2.2	Centerbase provides a process to employees for reporting security, confidentiality, integrity, and availability features, incidents, and concerns, and other complaints to company management.	Inspected the Company's intranet to determine whether Centerbase provided a process to employees for reporting security, confidentiality, integrity, and availability features, incidents, and concerns, and other complaints to company management.	No exceptions noted
	CC3.1.1	Centerbase has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the risk management policies and procedures to determine whether they specified risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	No exceptions noted

Section IV - Trust Services Category, Criteria, Related Controls, Tests, and Test Results

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

Trust Services Criteria	Control Ref #	Centerbase's Control Description	Test Procedure	Test Result
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.	CC6.1.1	Access to corporate network, production machines, network devices, and support tools requires a unique ID.	Inspected the login configuration to determine whether access to corporate network, production machines, network devices, and support tools required a unique ID.	No exceptions noted
	CC6.1.2	Centerbase ensures that all company-issued computers use a screensaver lock with a timeout of no more than 15 minutes.	Inspected the workstation configuration to determine whether all company-issued computers used a screensaver lock with a timeout of no more than 15 minutes.	No exceptions noted
	CC6.1.3	Centerbase authorizes access to information resources, including data and the systems that store or process sensitive data, based on the principle of least privilege.	Inspected the user listing to determine whether Centerbase authorized access to information resources, including data and the systems that store or process sensitive data, based on the principle of least privilege.	No exceptions noted
	CC6.1.4	Centerbase identifies, inventories, classifies, and assigns owners to IT assets.	Inspected the asset inventory to determine whether Centerbase identified, inventoried, classified, and assigned owners to IT assets.	No exceptions noted
	CC6.1.5	Centerbase performs annual access control reviews.	Inspected the access control review to determine whether it was completed annually by Centerbase.	No exceptions noted
	CC6.1.6	Read/write access to cloud data storage is configured to restrict public access.	Inspected the data storage configuration to determine whether read/write access to cloud data storage was configured to restrict public access.	No exceptions noted

Section IV - Trust Services Category, Criteria, Related Controls, Tests, and Test Results

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

Trust Services Criteria	Control Ref #	Centerbase's Control Description	Test Procedure	Test Result
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.	CC6.1.7	Centerbase requires two factor authentication to access sensitive systems and applications.	Inspected the login configuration to determine whether Centerbase required two factor authentication to access sensitive systems and applications.	No exceptions noted
	CC6.1.8	For changes to user privileges, user access requests are approved by IT management prior to being provisioned by a secondary member of the IT team.	Inspected access provisioning documentation for a selection of user access modifications to determine whether user access requests were approved by IT management prior to being provisioned by a secondary member of the IT team.	No exceptions noted
	CC6.1.9	Username and designated password configurations (password standard implemented) or SSO are required to authenticate into application.	Inspected the login configuration to determine whether username and password (password standard implemented) or SSO were required to authenticate into application.	No exceptions noted
	CC6.1.10	Centerbase automatically logs users out after a predefined inactivity interval and/or closure of the internet browser, and requires users to reauthenticate.	Inspected the login configuration to determine whether Centerbase automatically logged users out after a predefined inactivity interval and/or closure of the internet browser, and required users to reauthenticate.	No exceptions noted

Section IV - Trust Services Category, Criteria, Related Controls, Tests, and Test Results

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

Trust Services Criteria	Control Ref #	Centerbase's Control Description	Test Procedure	Test Result
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.	CC6.2.1	Centerbase has a defined system access control policy which outlines access requirements for the Company's in-scope systems. The policy is reviewed annually by management and made available to Centerbase personnel.	Inspected the system access control policy to determine whether it was in place, made available to Centerbase personnel, and reviewed annually by management.	No exceptions noted
	CC6.2.2	Appropriate levels of access to infrastructure and code review tools are granted to new employees within one week of their start date.	Inspected the access provisioning documentation for a selection of new hires to determine whether appropriate levels of access to infrastructure and code review tools were granted to new employees within one week of their start date.	No exceptions noted
	CC6.2.3	Firewall systems are in place to protect Centerbase's application from outside threats.	Inspected the firewall configuration to determine whether a firewall was in place to protect Centerbase's application from outside threats.	No exceptions noted
	CC6.1.3	Centerbase authorizes access to information resources, including data and the systems that store or process sensitive data, based on the principle of least privilege.	Inspected the user listing to determine whether Centerbase authorized access to information resources, including data and the systems that store or process sensitive data, based on the principle of least privilege.	No exceptions noted
	CC6.1.5	Centerbase performs annual access control reviews.	Inspected the access control review to determine whether it was completed annually by Centerbase.	No exceptions noted

Section IV - Trust Services Category, Criteria, Related Controls, Tests, and Test Results

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

Trust Services Criteria	Control Ref #	Centerbase's Control Description	Test Procedure	Test Result
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.	CC6.3.1	Centerbase uses a termination checklist to ensure that an employee's system access, including physical access, is removed within 24 hours and all organization assets (physical or electronic) are properly returned.	Inspected the termination checklists for a selection of terminated employees to determine whether access was removed within 24 hours, and organization assets were properly returned.	No exceptions noted
	CC6.3.2	SSH users use unique accounts to access production machines. Additionally, the use of the root account is not allowed.	Inspected the SSH users and authentication to determine whether a unique account was required in order to access production machines. Inspected root account authentication to determine that the use of the root account was not allowed.	No exceptions noted
	CC6.3.3	Users can only access the production system remotely through the use of encrypted communication systems.	Inspected the SSL certificates to determine whether users could only access the production system remotely through the use of encrypted communication systems.	No exceptions noted

Section IV - Trust Services Category, Criteria, Related Controls, Tests, and Test Results

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

Trust Services Criteria	Control Ref #	Centerbase's Control Description	Test Procedure	Test Result
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.	CC6.1.3	Centerbase authorizes access to information resources, including data and the systems that store or process sensitive data, based on the principle of least privilege.	Inspected the user listing to determine whether Centerbase authorized access to information resources, including data and the systems that store or process sensitive data, based on the principle of least privilege.	No exceptions noted
	CC6.1.5	Centerbase performs annual access control reviews.	Inspected the access control review to determine whether it was completed annually by Centerbase.	No exceptions noted
	CC6.1.8	For changes to user privileges, user access requests are approved by IT management prior to being provisioned by a secondary member of the IT team.	Inspected access provisioning documentation for a selection of user access modifications to determine whether user access requests were approved by IT management prior to being provisioned by a secondary member of the IT team.	No exceptions noted

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

Trust Services Criteria	Control Ref #	Centerbase's Control Description	Test Procedure	Test Result
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.	CC6.4.1	Annually, Centerbase reviews the third-party audit reports for data center subservice providers to evaluate the design and operating effectiveness of physical access and environmental controls.	Inspected the SOC report and management's review for the subservice organizations to determine whether management reviewed the third-party audit report/s for data center subservice providers to evaluate the design and operating effectiveness of physical access and environmental controls on an annual basis.	No exceptions noted
	CC6.4.2	Centerbase utilizes multiple availability zones to replicate production data across different zones.	Inspected the backup configuration to determine whether Centerbase utilized multiple availability zones to replicate production data across different zones.	No exceptions noted
	CC6.4.3	Centerbase has security policies that have been approved by management and detail how physical access to the Company's headquarters is maintained. These policies are accessible to all employees and contractors.	Inspected the security policies to determine whether they were approved by management and detailed how physical access to the Company's headquarters is maintained. Inspected the Company intranet to determine whether security policies were accessible to all employees and contractors.	No exceptions noted

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

Trust Services Criteria	Control Ref #	Centerbase's Control Description	Test Procedure	Test Result
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.	CC6.4.4	Physical access to the Centerbase colocation facility is approved by an authorized individual prior to being granted.	Inquired of management to understand the process by which physical access to the Centerbase colocation facility is approved by an authorized individual prior to being granted. Inspected the system generated listing of employees with access to the colocation facility to determine no new employees were granted access during the examination period.	Non-occurrence: Armanino is unable to opine on the operating effectiveness of the control as there was no new access granted to the colocation facility during the examination period.
	CC6.4.5	Physical access to the colocation facility is reviewed at least annually by management personnel.	Inspected the colocation facility access review to determine whether it was completed annually by management.	No exceptions noted
	CC6.3.1	Centerbase uses a termination checklist to ensure that an employee's system access, including physical access, is removed within 24 hours and all organization assets (physical or electronic) are properly returned.	Inspected the termination checklists for a selection of terminated employees to determine whether access was removed within 24 hours, and organization assets were properly returned.	No exceptions noted

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

Trust Services Criteria	Control Ref #	Centerbase's Control Description	Test Procedure	Test Result
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.	CC6.5.1	Centerbase has a documented policy for data retention defining the types of data (including company and customer data) and the period of time for which they should be retained.	Inspected the data protection policy to determine whether Centerbase had a documented policy for data retention defining the types of data (including company and customer data) and the period of time for which they should be retained.	No exceptions noted
	CC6.5.2	Centerbase deletes customer data within 30 days of the customer terminating its contract.	Inspected tickets for a selection of terminated customers to determine whether customer data was deleted within 30 days of termination.	No exceptions noted
	CC6.5.3	Centerbase disposes of hardcopy material with sensitive data when no longer needed (for legal or business reasons, or upon expiration of their retention period) through secure means such as cross-cut shredding, incinerating, or pulping, so that the data cannot be reconstructed.	Inquired of management to understand the process by which hardcopy data disposal requests are identified and tracked for evaluation. Inspected the manually maintained listing for hardcopy data disposal requests to determine there were no deletion requests during the examination period.	Non-occurrence: Armanino is unable to opine on the operating effectiveness of the control as there were no hardcopy data disposal requests during the examination period.
	CC6.5.4	Centerbase has formal policies and procedures in place to guide personnel in the disposal of hardware containing sensitive data.	Inspected the asset management policy to determine whether Centerbase had formal policies and procedures in place to guide personnel in the disposal of hardware containing sensitive data.	No exceptions noted

Section IV - Trust Services Category, Criteria, Related Controls, Tests, and Test Results

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

Trust Services Criteria	Control Ref #	Centerbase's Control Description	Test Procedure	Test Result
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	CC6.6.1	Centerbase requires antivirus software to be installed on workstations to protect the network against malware.	Inspected the antivirus configuration to determine whether Centerbase required antivirus software to be installed on workstations to protect the network against malware.	No exceptions noted
	CC6.6.2	Centerbase ensures that all connections to its web application from its users are encrypted.	Inspected the web application configuration to determine whether all data in transits was encrypted.	No exceptions noted
	CC6.1.6	Read/write access to cloud data storage is configured to restrict public access.	Inspected the data storage configuration to determine whether read/write access to cloud data storage was configured to restrict public access.	No exceptions noted
	CC6.1.7	Centerbase requires two factor authentication to access sensitive systems and applications.	Inspected the login configuration to determine whether Centerbase required two factor authentication to access sensitive systems and applications.	No exceptions noted
	CC6.1.9	Username and designated password configurations (password standard implemented) or SSO are required to authenticate into application.	Inspected the login configuration to determine whether username and password (password standard implemented) or SSO were required to authenticate into application.	No exceptions noted
	CC6.3.3	Users can only access the production system remotely through the use of encrypted communication systems.	Inspected the SSL certificates to determine whether users could only access the production system remotely through the use of encrypted communication systems.	No exceptions noted

Section IV - Trust Services Category, Criteria, Related Controls, Tests, and Test Results

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

Trust Services Criteria	Control Ref #	Centerbase's Control Description	Test Procedure	Test Result
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.	CC6.7.1	The use of removable media is restricted by policy.	Inspected the removable media configuration to determine whether company-issued removable media devices (USB drives) were encrypted.	No exceptions noted
	CC6.7.2	Centerbase ensures that company-issued laptops have encrypted hard-disks.	Inspected the workstation configuration to determine whether all company-issued computers had encrypted hard-disks.	No exceptions noted
	CC6.7.3	Centerbase has an established key management process in place to support the organization's use of cryptographic techniques.	Inspected the key management tool to determine whether it was in place to support the organization's use of cryptographic techniques.	No exceptions noted
	CC6.7.4	Centerbase stores data in databases that is encrypted at rest.	Inspected the databases to determine whether all data was encrypted at rest.	No exceptions noted
	CC6.3.2	SSH users use unique accounts to access production machines. Additionally, the use of the root account is not allowed.	Inspected the SSH users and authentication to determine whether a unique account was required in order to access production machines. Inspected root account authentication to determine that the use of the root account was not allowed.	No exceptions noted
	CC6.3.3	Users can only access the production system remotely through the use of encrypted communication systems.	Inspected the SSL certificates to determine whether users could only access the production system remotely through the use of encrypted communication systems.	No exceptions noted

Section IV - Trust Services Category, Criteria, Related Controls, Tests, and Test Results

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

Trust Services Criteria	Control Ref #	Centerbase's Control Description	Test Procedure	Test Result
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.	CC6.8.1	Centerbase has implemented tools to monitor Centerbase's databases and servers and notify appropriate personnel of any events or incidents based on predetermined criteria.	Inspected the monitoring tools to determine whether Centerbase had implemented tools to monitor Centerbase's databases and notify appropriate personnel of any events or incidents based on predetermined criteria.	No exceptions noted
	CC5.1.2	Centerbase's workstations operating system (OS) security patches are applied automatically.	Inspected the mobile device management configuration to determine whether Centerbase's workstations operating system (OS) security patches were applied automatically.	No exceptions noted
	CC6.6.1	Centerbase requires antivirus software to be installed on workstations to protect the network against malware.	Inspected the web application configuration to determine whether all data in transits was encrypted.	No exceptions noted
	CC6.7.2	Centerbase ensures that company-issued laptops have encrypted hard-disks.	Inspected the workstation configuration to determine whether all company-issued computers had encrypted hard-disks.	No exceptions noted

Section IV - Trust Services Category, Criteria, Related Controls, Tests, and Test Results

CC7.0 Common Criteria Related to System Operations

Trust Services Criteria	Control Ref #	Centerbase's Control Description	Test Procedure	Test Result
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.	CC7.1.1	Centerbase has infrastructure logging configured to monitor web traffic and suspicious activity. When anomalous traffic activity is identified, alerts are automatically created, sent to appropriate personnel and resolved, as necessary.	Inspected the logging tool to determine whether Centerbase had infrastructure logging configured to monitor web traffic and suspicious activity. Inspected the alert configuration to determine whether anomalous traffic activity was identified, alerts were automatically created, and sent to appropriate personnel and resolved, as necessary.	No exceptions noted
	CC7.1.2	An intrusion detection system (IDS) is in place to detect potential intrusions, alert personnel when a potential intrusion is detected	Inspected the intrusion detection system to determine whether it was in place to detect potential intrusions, alert personnel when a potential intrusion is detected	No exceptions noted
	CC3.2.3	Centerbase engages with a third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management.	Inspected the vulnerability scans for a selection of quarters to determine whether the scan was completed on a quarterly basis.	No exceptions noted
			Inspected the IT management meeting documentation to determine whether results were reviewed by management.	No exceptions noted

CC7.0 Common Criteria Related to System Operations

Trust Services Criteria	Control Ref #	Centerbase's Control Description	Test Procedure	Test Result
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.	CC3.2.4	Centerbase engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.	Inspected the penetration test to determine whether it was completed on an annual basis. Inspected the penetration test review documentation to determine whether the penetration test was reviewed by management and high priority findings are tracked to resolution.	No exceptions noted

Section IV - Trust Services Category, Criteria, Related Controls, Tests, and Test Results

CC7.0 Common Criteria Related to System Operations

Trust Services Criteria	Control Ref #	Centerbase's Control Description	Test Procedure	Test Result
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.	CC7.2.1	Centerbase tracks and prioritizes security deficiencies through internal tools according to their severity by an independent technical resource.	Inquired of management to understand the process by which Centerbase tracks and prioritizes security deficiencies through internal tools according to severity. Inspected the system generated listing of security deficiencies to determine no security deficiencies were noted during the examination period.	Non-occurrence: Armanino is unable to opine on the operating effectiveness of the control as there were no security deficiencies during the examination period.
	CC7.2.2	Centerbase has implemented an incident response plan that includes creating, prioritizing, assigning, and tracking follow-ups to completion and lend support to business continuity/disaster recovery.	Inspected the incident management policies to determine whether had implemented an incident response plan that includes creating, prioritizing, assigning, and tracking follow-ups to completion and lend support to business continuity/disaster recovery.	No exceptions noted
	CC7.2.3	Centerbase uses logging software that sends alerts to appropriate personnel. Corrective actions are performed, as necessary, in a timely manner.	Inspected the logging tool to determine whether Centerbase had infrastructure logging configured to monitor web traffic and suspicious activity. Inspected the alert configuration to determine whether anomalous traffic activity was identified, alerts were automatically created, and sent to appropriate personnel and resolved, as necessary.	No exceptions noted

Section IV - Trust Services Category, Criteria, Related Controls, Tests, and Test Results

CC7.0 Common Criteria Related to System Operations

Trust Services Criteria	Control Ref #	Centerbase's Control Description	Test Procedure	Test Result
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.	CC7.2.4	Centerbase has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the Company.	Inspected the incident management policies to determine whether Centerbase had identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the Company.	No exceptions noted
	CC3.2.3	Centerbase engages with a third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management.	Inspected the vulnerability scans for a selection of quarters to determine whether the scan was completed on a quarterly basis.	No exceptions noted
			Inspected the IT management meeting documentation to determine whether results were reviewed by management.	No exceptions noted

CC7.0 Common Criteria Related to System Operations

Trust Services Criteria	Control Ref #	Centerbase's Control Description	Test Procedure	Test Result
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.	CC3.2.4	Centerbase engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.	Inspected the penetration test to determine whether it was completed on an annual basis. Inspected the penetration test review documentation to determine whether the penetration test was reviewed by management and high priority findings are tracked to resolution.	No exceptions noted
	CC6.8.1	Centerbase has implemented tools to monitor Centerbase's databases and servers and notify appropriate personnel of any events or incidents based on predetermined criteria. Incidents are escalated per policy.	Inspected the monitoring tools to determine whether Centerbase had implemented tools to monitor Centerbase's databases and notify appropriate personnel of any events or incidents based on predetermined criteria.	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.	CC7.3.1	Centerbase tracks security deficiencies through internal tools and closes them within an SLA that management has pre-specified.	Inquired of management to understand the process by which Centerbase tracks security deficiencies through internal tools and closes them within an SLA that management has pre-specified. Inspected the system generated listing of security deficiencies to determine no security deficiencies were noted during the examination period.	Non-occurrence: Armanino is unable to opine on the operating effectiveness of the control as there were no security deficiencies during the examination period.

CC7.0 Common Criteria Related to System Operations

Trust Services Criteria	Control Ref #	Centerbase's Control Description	Test Procedure	Test Result
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.	CC7.3.2	Centerbase has implemented an incident response plan that includes documenting lessons learned and "root cause analysis" after incidents and sharing them with the broader engineering team to support business continuity/disaster recovery.	Inquired of management to understand the process by which Centerbase documents lessons learned and root cause analysis after incidents. Inspected the system generated listing of security deficiencies to determine no security deficiencies were noted during the examination period.	Non-occurrence: Armanino is unable to opine on the operating effectiveness of the control as there were no security deficiencies during the examination period.
	CC7.2.1	Centerbase tracks and prioritizes security deficiencies through internal tools according to their severity by an independent technical resource.	Inquired of management to understand the process by which Centerbase tracks and prioritizes security deficiencies through internal tools according to severity. Inspected the system generated listing of security deficiencies to determine no security deficiencies were noted during the examination period.	Non-occurrence: Armanino is unable to opine on the operating effectiveness of the control as there were no noted security deficiencies during the examination period.
	CC7.2.2	Centerbase has implemented an incident response plan that includes creating, prioritizing, assigning, and tracking follow-ups to completion and lend support to business continuity/disaster recovery.	Inspected the incident management policies to determine whether had implemented an incident response plan that includes creating, prioritizing, assigning, and tracking follow-ups to completion and lend support to business continuity/disaster recovery.	No exceptions noted

CC7.0 Common Criteria Related to System Operations

Trust Services Criteria	Control Ref #	Centerbase's Control Description	Test Procedure	Test Result
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.	CC7.2.4	Centerbase has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the Company.	Inspected the incident management policies to determine whether Centerbase had identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the Company.	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.	CC7.2.1	Centerbase tracks and prioritizes security deficiencies through internal tools according to their severity by an independent technical resource.	Inquired of management to understand the process by which Centerbase tracks and prioritizes security deficiencies through internal tools according to severity. Inspected the system generated listing of security deficiencies to determine no security deficiencies were noted during the examination period.	Non-occurrence: Armanino is unable to opine on the operating effectiveness of the control as there were no security deficiencies during the examination period.
	CC7.2.2	Centerbase has implemented an incident response plan that includes creating, prioritizing, assigning, and tracking follow-ups to completion and lend support to business continuity/disaster recovery.	Inspected the incident management policies to determine whether had implemented an incident response plan that includes creating, prioritizing, assigning, and tracking follow-ups to completion and lend support to business continuity/disaster recovery.	No exceptions noted

CC7.0 Common Criteria Related to System Operations

Trust Services Criteria	Control Ref #	Centerbase's Control Description	Test Procedure	Test Result
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.	CC7.2.4	Centerbase has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the Company.	Inspected the incident management policies to determine whether Centerbase had identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the Company.	No exceptions noted
CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.	CC7.5.1	Centerbase has an established disaster recovery plan that outlines roles and responsibilities and detailed procedures for recovery of systems.	Inspected the disaster recovery plan to determine whether it outlined roles and responsibilities and detailed procedures for recovery of systems.	No exceptions noted
	CC7.5.2	Centerbase performs backups daily and retains them in accordance with a predefined schedule in the backup policy.	Inspected the backup configuration to determine whether backups were performed daily and were retained in accordance with a predefined schedule in the Backup Policy.	No exceptions noted
	CC7.5.3	Centerbase conducts annual BCP/DR tests and documents according to the BCDR Plan.	Inspected the BCP and DR test to determine whether the test was completed on an annual basis.	No exceptions noted

Section IV - Trust Services Category, Criteria, Related Controls, Tests, and Test Results

CC7.0 Common Criteria Related to System Operations

Trust Services Criteria	Control Ref #	Centerbase's Control Description	Test Procedure	Test Result
CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.	CC7.5.4	Centerbase has a defined business continuity plan that outlines the proper procedures to respond, recover, resume, and restore operations following a disruption or significant change.	Inspected the business continuity plan to determine whether it outlined the proper procedures to respond, recover, resume, and restore operations following a disruption or significant change.	No exceptions noted
	CC7.2.1	Centerbase tracks and prioritizes security deficiencies through internal tools according to their severity by an independent technical resource.	Inquired of management to understand the process by which Centerbase tracks and prioritizes security deficiencies through internal tools according to severity. Inspected the system generated listing of security deficiencies to determine no security deficiencies were noted during the examination period.	Non-occurrence: Armanino is unable to opine on the operating effectiveness of the control as there were no security deficiencies during the examination period.

CC8.0 Common Criteria Related to Change Management

Trust Services Criteria	Control Ref #	Centerbase's Control Description	Test Procedure	Test Result
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.	CC8.1.1	Centerbase has developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating changes.	Inspected the change management policy to determine whether it governed the system development life cycle, including documented policies for tracking, testing, approving, and validating changes.	No exceptions noted
	CC8.1.2	When Centerbase's application code changes, code reviews and tests are performed by someone other than the person who made the code change.	Inspected the change documentation for a selection of application changes to determine whether code reviews and testing were completed by someone other than the person who made the code change.	No exceptions noted
	CC8.1.3	Centerbase ensures that code changes are tested prior to deployment to ensure quality and security.	Inspected the change documentation for a selection of application changes to determine whether code changes were tested prior to deployment to ensure quality and security.	No exceptions noted
	CC8.1.4	Separate environments are used for testing and production for Centerbase's application.	Inspected the Company's environments to determine whether separate environments were used for testing and production for Centerbase's application.	No exceptions noted
	CC8.1.5	Only authorized Centerbase personnel can push or make changes to production code.	Inspected the user listing to determine whether only authorized Centerbase personnel can push or make changes to production code.	No exceptions noted

CC8.0 Common Criteria Related to Change Management

Trust Services Criteria	Control Ref #	Centerbase's Control Description	Test Procedure	Test Result
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.	CC8.1.6	Centerbase ensures that releases are approved by appropriate members of management prior to production release.	Inspected change documentation for a selection of releases to determine whether each release was approved by appropriate members of management prior to production release.	No exceptions noted
	CC8.1.7	Centerbase uses a version control system to manage source code, documentation, release labeling, and other change management tasks.	Inspected the version control system to determine it was used to manage source code, documentation, release labeling, and other change management tasks.	No exceptions noted
	CC8.1.8	On a quarterly basis, management performs a comparison of change deployments against the corresponding change approvals to ensure no changes circumvented the change approval process.	Inspected change documentation for a selected quarter to determine whether management performed a comparison of change deployments against the corresponding change approvals to ensure no changes circumvented the change approval process.	No exceptions noted

Section IV - Trust Services Category, Criteria, Related Controls, Tests, and Test Results

CC9.0 Common Criteria Related to Risk Mitigation

Trust Services Criteria	Control Ref #	Centerbase's Control Description	Test Procedure	Test Result
CC9.1 - The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	CC9.1.1	Centerbase maintains cybersecurity insurance to mitigate the financial impact of business disruptions.	Inspected the cybersecurity insurance to determine whether it was in place to mitigate the financial impact of business disruptions.	No exceptions noted
	CC3.1.1	Centerbase has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the risk management policies and procedures to determine whether they specified risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	No exceptions noted
	CC3.2.1	Centerbase's management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Inspected the risk assessment documentation to determine whether management prepared a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	No exceptions noted
	CC7.5.1	Centerbase has an established disaster recovery plan that outlines roles and responsibilities and detailed procedures for recovery of systems.	Inspected the disaster recovery plan to determine whether it outlined roles and responsibilities and detailed procedures for recovery of systems.	No exceptions noted
	CC7.5.3	Centerbase conducts annual BCP/DR tests and documents according to the BCDR Plan.	Inspected the BCP and DR test to determine whether the test was completed on an annual basis.	No exceptions noted

CC9.0 Common Criteria Related to Risk Mitigation

Trust Services Criteria	Control Ref #	Centerbase's Control Description	Test Procedure	Test Result
CC9.2 - The entity assesses and manages risks associated with vendors and business partners.	CC9.2.1	As part of the third-party vendor management process, management periodically reviews the performance of vendor entities. Vendor reviews are completed by the Information Security team, and instances of vendor non-compliance are reported to the management team as they are discovered.	Inspected vendor reviews for a selection of new vendors to determine whether management reviews the performance of vendor entities.	Exception noted: For 4 of 4 non-critical vendors sampled, Armanino noted a vendor review had not been performed within the last 12 months.
	CC9.2.2	Centerbase's new hire contracts include a non-disclosure agreement (NDA)	Inspected the contracts for a selection of new hires to determine whether each signed contract included an NDA.	No exceptions noted
	CC9.2.3	Centerbase has a defined vendor management policy that establishes requirements of ensuring third-party entities meet the organization's data preservation and protection requirements.	Inspected the vendor management policy to determine whether it established requirements of ensuring third-party entities meet the organization's data preservation and protection requirements.	No exceptions noted

Section IV - Trust Services Category, Criteria, Related Controls, Tests, and Test Results

CC9.0 Common Criteria Related to Risk Mitigation

Trust Services Criteria	Control Ref #	Centerbase's Control Description	Test Procedure	Test Result
CC9.2 - The entity assesses and manages risks associated with vendors and business partners.	CC6.4.1	Annually, Centerbase reviews the third-party audit reports for data center subservice providers to evaluate the design and operating effectiveness of physical access and environmental controls.	Inspected the SOC report and management's review for the subservice organizations to determine whether management reviewed the third-party audit report/s for data center subservice providers to evaluate the design and operating effectiveness of physical access and environmental controls on an annual basis.	No exceptions noted

Section V – Other Information Provided by Management Not Covered by the Service Auditor's Report

Management's Responses to Noted Exceptions

Control Ref #	Company's Control Description	Exception Noted	Management Response
CC1.1.3	Company policies are accessible to all employees and, as appropriate, third parties. Personnel are required to acknowledge the information security policy and other topic-specific policies based on their job duties during onboarding and annually thereafter.	For 2 of 3 new hires sampled, the information security policy was not acknowledged within 30 days of hire.	Centerbase has incorporated the information security policy into each employee's Drata dashboard with automated follow up to ensure more thorough completion.
		For 10 of 12 existing employees sampled, annual re-acknowledgment of the information security had not been performed within the last 12 months.	Centerbase has incorporated the information security policy into each employee's Drata dashboard with automated follow up to ensure more thorough completion.
CC1.4.2	Centerbase has established training programs for privacy and information security to help employees understand their obligations and responsibilities to comply with Centerbase's security policies and procedures, including the identification and reporting of incidents. All full-time employees are required to complete the training upon hire and annually thereafter.	For 3 of 3 new hires sampled, security training was not completed within 30 days of hire.	Centerbase has incorporated security training into each employee's Drata dashboard with automated follow up to ensure more thorough completion.
		For 2 of 12 existing employees sampled, security training had not been completed within the last 12 months.	Centerbase has incorporated security training into each employee's Drata dashboard with automated follow up to ensure more thorough completion.

Section V – Other Information Provided by Management Not Covered by the Service Auditor's Report

Management's Responses to Noted Exceptions

Control Ref #	Company's Control Description	Exception Noted	Management Response
CC1.5.1	Centerbase evaluates the performance of all employees through a formal, annual performance evaluation.	For 1 of 12 existing employees sampled, a performance evaluation had not been performed within the last 12 months.	Due to extenuating circumstances, this employee did not have a performance review but has since received one and will continue to receive them quarterly.
CC5.1.1	Centerbase ensures that virtual machine OS patches are applied quarterly.	For 1 of 10 virtual machines sampled, patching had not been performed for the quarter tested.	The virtual machine in question was in the FLS environment, going into service in May 2024, and has since been updated and will be automatically updated moving forward.
CC9.2.1	As part of the third-party vendor management process, management periodically reviews the performance of vendor entities. Vendor reviews are completed by the Information Security team, and instances of vendor non-compliance are reported to the management team as they are discovered.	For 4 of 4 non-critical vendors sampled, Armanino noted a vendor review had not been performed within the last 12 months.	Centerbase has begun leveraging Drata to ensure that all vendor reviews are completed in a timely manner.