linford&co llp
cpa firm

sugarcrm

TYPE II SOC 2

REPORT ON CONTROLS RELEVANT TO SECURITY

MARCH 1, 2023 TO FEBRUARY 29, 2024

SugarCRM Inc.

Report on SugarCRM's Description of Its SugarCRM Platform and on Its Controls Relevant to Security

Table of Contents

SugarCRM Inc.

Report on SugarCRM's Description of Its SugarCRM Platform and on Its Controls Relevant to Security

Table of Contents (continued)

linford&co llp
cpa firm

linford&co llp
1550 wewatta st, 2nd floor
denver, co 80202

tel: +1 (720) 330 7201
email: info@linfordco.com
www.linfordco.com

Section I – Independent Service Auditor's Report

To the Management of SugarCRM Inc.:

Scope

We have examined SugarCRM Inc.'s (SugarCRM or the Company) accompanying description of its SugarCRM platform titled, "SugarCRM's Description of Its SugarCRM Platform" throughout the period March 1, 2023 to February 29, 2024 (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (AICPA, *Description Criteria*) (description criteria), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period March 1, 2023 to February 29, 2024 to provide reasonable assurance that SugarCRM's service commitments and system requirements were achieved based on the trust services criteria relevant to security set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

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

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

Service Organization's Responsibilities

SugarCRM 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 SugarCRM's service commitments and system requirements were achieved. SugarCRM has provided the accompanying assertion titled, "Assertion of SugarCRM Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. SugarCRM 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 (AICPA). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

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

- ✓ Obtaining an understanding of the system and 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 users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of 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 and 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 presented in Section IV of this report titled, *Independent Service Auditor's Description of Tests of Controls and Results*.

Opinion

In our opinion, in all material respects:

a. The description presents the Company's SugarCRM platform that was designed and implemented throughout the period March 1, 2023 to February 29, 2024 in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period March 1, 2023 to February 29, 2024 to provide reasonable assurance that SugarCRM's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organization and user entities applied the complementary controls assumed in the design of SugarCRM's controls throughout that period.
c. The controls stated in the description operated effectively throughout the period March 1, 2023 to February 29, 2024 to provide reasonable assurance that SugarCRM'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 SugarCRM'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 SugarCRM, user entities of the Company's SugarCRM platform during some or all of the period March 1, 2023 to February 29, 2024, business partners of SugarCRM subject to risks arising from interactions with the SugarCRM platform, 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 these specified parties.

linford&co llp

March 1, 2024
Denver, Colorado

SugarCRM Inc.
10050 North Wolfe Road, SW2-130
Cupertino, CA 95014
877.842.7276

Section II – Assertion of SugarCRM Management

March 1, 2024

We have prepared the accompanying description of SugarCRM Inc.'s (SugarCRM or the Company) SugarCRM platform titled, "SugarCRM's Description of Its SugarCRM Platform" throughout the period March 1, 2023 to February 29, 2024 (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (AICPA, *Description Criteria*) (description criteria). The description is intended to provide report users with information about the SugarCRM platform that may be useful when assessing the risks arising from interactions with SugarCRM's system, particularly information about system controls that SugarCRM 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 set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

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

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

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

a) The description presents the Company's SugarCRM platform that was designed and implemented throughout the period March 1, 2023 to February 29, 2024 in accordance with the description criteria.
b) The controls stated in the description were suitably designed throughout the period March 1, 2023 to February 29, 2024 to provide reasonable assurance that SugarCRM's service commitments and

SugarCRM Inc.
10050 North Wolfe Road, SW2-130
Cupertino, CA 95014
877.842.7276

system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of SugarCRM's controls throughout that period.

c) The controls stated in the description operated effectively throughout the period March 1, 2023 to February 29, 2024 to provide reasonable assurance that SugarCRM'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 SugarCRM's controls operated effectively throughout that period.

Craig Barber
Chief Information Security Officer

Section III – SugarCRM's Description of Its SugarCRM Platform

Overview of Operations

Overview of the Organization: SugarCRM is an industry-leading company focused exclusively on customer relationship management (CRM). SugarCRM is headquartered in Cupertino, California. Since 2004, SugarCRM has been helping its clients create better relationships with their customers. The Company is recognized by leading market analysts as a CRM innovator. The SugarCRM platform is deployed by more than 2 million individuals in over 120 countries and 26 languages. Companies large and small are turning from yesterday's CRM solutions to rely on SugarCRM to manage customer relationships.

Description of the SugarCRM Platform and Services

SugarCRM enables its clients to create extraordinary customer relationships through the use of its CRM solution: the SugarCRM platform. The SugarCRM platform is an affordable CRM that is easily customizable for any business' needs to empower their personnel to become customer experts and grow the business. The following summarizes the components of the SugarCRM platform and the services each provides to SugarCRM's clients:

- *Sugar Market:* Sugar Market is designed to help users through awareness, interest, and consideration stages of the customer relationship cycle. Sugar Market provides users with a curated toolset that includes highly intuitive campaign builders, advanced automations, and superior reporting to help streamline campaign creation, increase engagement, and improve conversion.
- *Sugar Sell:* Sugar Sell focuses on the consideration, purchase, and retention stages of the customer relationship cycle. It improves sales representatives' efficiency by capturing and organizing information, prioritizing activities and workload, providing the relevant prospect information when needed, and managing the sales process through closure. Sugar Sell provides managers with the necessary information to understand an organization's sales pipeline to be able to more accurately forecast sales and measure individual and organizational performance.
- *Sugar Serve:* Sugar Serve is an innovative customer service center for multi-channel case management and customer service. Focusing on the retention and advocacy stages of the customer relationship cycle, Sugar Serve helps customer service agents and managers prioritize, track, and resolve support cases efficiently. Designed to reduce case response and resolution times, the ultimate goal of Sugar Sell is to reduce service costs while increasing customer satisfaction and building trusted relationships with customers.
- *Sugar Discover:* Sugar Discover is an advanced analytics tool that provides users with accurate, relevant information from activities across the entire customer relationship cycle. Sugar Discover provides operational reports, descriptive analytics, and historical analysis that enables users to identify potential issues within their pipeline or individual performance. The business intelligence is pre-integrated. Users can use out-of-the box analytics and reporting without the need for data modeling, data warehouses, or data scientists.

- *Sugar Hint:* Sugar Hint is a sales intelligence tool designed to increase productivity and provide rich contextual data about customers that helps reduce the amount of time spent by sales personnel identifying, researching, and preparing for opportunities. Sugar Hint supplements users' company data from more than 100 different public sources. It also provides relevant breaking news about customers so that users can take action at the right time to have more productive meetings. Users can also use these features to enhance its interactions with their current customers.
- *Sugar Connect:* Sugar Connect allows users to extend key customer information and coordinate activities, contacts, and information with Office 365 and Google Workspace. Users can access customer information from Sugar Sell while in Outlook without having to switch applications simply by synchronizing calendar, tasks, and contacts.

Principal Service Commitments and System Requirements

SugarCRM designs its processes and procedures to meet objectives for its SugarCRM platform. Those objectives are based on the service commitments that SugarCRM makes to user entities and the compliance requirements that SugarCRM has established for its services.

Security commitments to user entities are documented and communicated in their customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental design of the SugarCRM platform are implemented to permit system users access to the information they need based on their role in the system while restricting them from accessing information not needed for their role.
- Controlled access to the platform and the supporting infrastructure.
- Segregation of client data.
- Monitoring of system performance metrics and critical application services.

SugarCRM establishes operational requirements that support the achievement of security commitments and other system requirements. Such requirements are communicated in the SugarCRM platform policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal networks are managed, and how employees are hired and trained.

Components of the System Used to Provide the Services

The system used by SugarCRM to deliver the SugarCRM platform and related services is comprised of a combination of components that include the platform itself and the data processed, but also extends to the underlying infrastructure, subservice organization's services supporting the platform, the Company's employees and contractors, as well as the policies and procedures followed to maintain the security of the SugarCRM platform and client data. The following is a summary of the components that comprise the

system. Specific processes and controls relevant to the security criteria are described in the remainder of this section of the report.

Infrastructure: SugarCRM uses AWS, a subservice organization, to provide cloud hosting services. AWS hosts SugarCRM's production IT environment. The facilities, including the hardware and equipment therein, are maintained by AWS. The physical security, environmental control, and incident management for the facilities is also the responsibility of AWS. SugarCRM is responsible for the configuration and maintenance of its cloud environment. The Company configures firewall protections through security groups and data backups in the AWS environment. AWS undergoes an annual SOC 2 Type II examination and the report may be obtained directly from them. SugarCRM obtains and reviews the SOC 2 report provided by AWS related to their hosting operations to determine whether controls are designed and operating effectively at AWS. Additionally, any listed complementary user entity controls in the AWS SOC reports are also reviewed and addressed by SugarCRM.

Software: The SugarCRM platform is the industry's only no-touch, time-aware customer experience platform. The platform is a proprietary solution owned by SugarCRM. The platform is developed and maintained by SugarCRM's in-house IT and engineering personnel. SugarCRM follows defined processes to manage changes to the platform. SugarCRM's access to the platform is governed by the principle of least privilege and is limited to authorized personnel.

People: SugarCRM personnel are organized into functional areas to facilitate efficient operations and clear divisions of responsibilities. The Company provides annual job trainings to help personnel understand their responsibilities and to maintain security within the organization.

Data: Client data is stored within the SugarCRM production database instance. SugarCRM has implemented security controls to protect the security and confidentiality of the data. Client data within the databases is encrypted at rest. Additionally, all data transfers between users and SugarCRM are secured using Transport Layer Security (TLS) and industry-standard encryption.

Processes and Procedures: SugarCRM maintains security policies and procedures for activities within the organization to maintain the security of the SugarCRM platform and related services. SugarCRM makes these internal policies and procedures, including security policies, available to its personnel on its intranet to provide direction regarding their responsibilities related to the functioning of internal control. Policies are reviewed regularly and updated as necessary.

Relevant Aspects of the Control Environment, Risk Assessment, Information and Communication, Monitoring, and Control Activities for the Security Criteria

Note: Parenthetical references have been included in the following narratives as a cross reference to the applicable control activities included in Section IV of this report.

A company's entity-level control reflects the overall attitude, awareness, and actions of management and others concerning the importance of controls and the emphasis given to controls in the company's policies, procedures, methods, and organizational structure. The entity-level controls are not specific to any individual transaction but apply to the company as a whole. These types of controls are necessary to facilitate the proper functioning of activity-level controls supporting the SugarCRM platform. This section contains a description of the five components of internal control (control environment, risk assessment, information and communication, monitoring, and control activities) as they relate to the platform SugarCRM provides to its clients.

The controls supporting the specified criteria were used to evaluate the suitability of design and operating effectiveness of controls stated in the description. Controls designed, implemented, and operated to meet them help determine whether the system is protected against unauthorized access (both physical and logical). Entity-level controls and specific control activities supporting the applicable trust services criteria are provided in the descriptions of this section of the report, and in *Section IV – Independent Service Auditor's Description of Tests of Controls and Results.*

Control Environment

The control environment is the umbrella under which all of the control components of internal control fall. The control environment at SugarCRM includes "tone at the top," which management sets by example in adhering to ethical business practices and company policies, and by conducting business with integrity. Management's example and leadership are the primary mechanisms used to guide employees in the execution of SugarCRM's operations. The control environment is the collective responsibility of the management team.

Commitment to Competence: SugarCRM's hiring practices are designed to facilitate the hiring of competent personnel in order to provide clients the highest quality of services. Candidates are carefully identified and interviewed by the management team before being considered for hire. Applicants selected for employment who will have access to sensitive client data are subject to background screenings. This helps SugarCRM maintain a stable and competent workforce, allowing management to focus on client service. SugarCRM provides employee onboarding to help new personnel assimilate quickly and contribute in key roles. SugarCRM also provides training to current employees to maintain their competencies.

Board of Directors: The Board of Directors consists of the founder of the company, the CEO, and members of the primary investment firm. The Board meets quarterly throughout the year to review the organization's

products and services provided to clients, business strategy, financial information, and other items that are related to the enterprise as a whole **(1.1)**. The Board plays an important role in the oversight and governance of the enterprise. The Board helps to monitor whether the enterprise is operating within established parameters and is complying with sound business practices.

Management Philosophy and Operating Style: Management understands the importance of oversight and governance and believes this is best accomplished when executives are highly involved in the day-to-day operations of SugarCRM. In this environment, management is able to address business issues in a timely manner and, consequently, reduce risks to the company and clients. Management and employees meet regularly to discuss system requirements and progress against outstanding deadlines. Individual performance is assessed periodically and communicated to employees by members of the management team. SugarCRM's expectations for all employees to conduct themselves honestly and ethically are communicated in the Company's code of conduct **(1.2)**.

A properly defined organizational structure is critical for operating a sound control environment. SugarCRM's organizational structure defines authorities across the Company to facilitate information flow and establish responsibilities **(1.3)**. In addition, lines of authority are clearly established throughout SugarCRM. These lines of authority are communicated through management's operational style, organizational structure, and employee job descriptions. To increase the operational effectiveness of employees within this structure, every position has a job description so individuals understand their roles and responsibilities **(1.4)**.

New Hires and Terminations: When a position is open at SugarCRM, a job description will be posted within SugarCRM's applicant tracking system. The positions are also posted online to various job forums. Resumes of candidates are received and initially screened by Human Resources (HR). Resumes that pass HR's initial screening are submitted to the hiring manager or supervisor for consideration. Interviews for individuals selected by the hiring manager or supervisor are scheduled and conducted. HR conducts additional screening of prior employment and education.

Applicants for full-time SugarCRM employment participate in a number of interviews, based on the position they are applying for. During the resume review and the interview process, technical competence is evaluated for selected candidates by the interviewer **(1.5)**. Integrity and ethical values are emphasized during the hiring and onboarding process.

Once a qualified candidate is selected internally, an offer letter and a consent for a background check are sent to the applicant for acceptance. Applicants for full-time SugarCRM employment are required to consent to and complete a successful background check. Applicants for employment at SugarCRM are screened to determine whether past behavior aligns with company policies and procedures **(1.6)**. New hires are required to review and sign the SugarCRM employee handbook (U.S. personnel) or the employment agreement (non-U.S. personnel), confidentiality agreement, and security policies to evidence that they will abide by the company policies as outlined in the provided documents **(1.7)**. The organizational values and behavioral standards at SugarCRM are built into the day-to-day activities. Management leads by example and encourages ethical behavior in all aspects of the business.

SugarCRM managers are actively involved in managing and evaluating the performance of their staff. Direct supervisors complete performance reviews for their staff through a series of questions and direct observation of performance. After the first year of employment, performance reviews occur at least annually **(1.8)**. Where needed, supervisors will provide additional monitoring to support performance improvement. Employees who do not meet expectations for the position they are hired for and who do not improve their performance through additional monitoring are terminated. If it is determined that an employee needs to be involuntarily terminated from SugarCRM, a termination letter is prepared and provided to the employee. For voluntary terminations, the employee separating submits a resignation letter. HR creates the exit paperwork, completes an exit interview, and obtains any assets from the employee. HR sends a termination notification to the help desk to have all access removed, as well as to other appropriate individuals within the Company.

Employee Training: To assist with SugarCRM's commitments to security, SugarCRM management provides mandatory security awareness training for new hires and annually each year thereafter **(1.9)**. The training covers General Data Protection Regulation (GDPR), information security, data protection, and maintaining confidentiality of client data. SugarCRM management tracks which employees have attended the annual security awareness training and the date(s) of completion.

Contractor Confidentiality: SugarCRM employs contracting agencies to recruit talents across the globe. Consulting agreements with contracting agencies address confidentiality of proprietary and confidential information of SugarCRM **(1.10)**.

Information and Communication

SugarCRM maintains internal documentation that specifies the Company's security policies to communicate certain responsibilities to SugarCRM personnel and system boundaries, which helps them understand their roles within the organization **(2.1)**. The policy highlights important internal controls that strengthen SugarCRM's overall control environment.

SugarCRM has an organizational reporting structure with defined reporting lines and authority hierarchy that delineates roles and responsibilities **(2.2)**. See the *Control Environment* section for additional details.

SugarCRM has also created a high-level overview of its SugarCRM platform used to describe the services provided to the clients that the SugarCRM platform serves **(2.3)**. This information is accessible on the Company's website, sugarcrm.com/solutions. The SugarCRM platform enables clients to collect critical information across sales, service, and marketing in order to provide their employees with the right information at the right time. SugarCRM and its clients' responsibilities and commitments regarding the acceptable use of the SugarCRM platform are included within the Master Subscription Agreement (MSA), which clients must agree to before using the SugarCRM platform **(2.4)**.

To assist with SugarCRM's commitments to security, SugarCRM management provides annual training for employees that covers information security and data protection **(2.5)**. SugarCRM includes GDPR in its

training program in order to better monitor that the employees working in the production environment are aware of data protection requirements and implementing appropriate safeguards to support data protection, as well as their understanding of data protection rules and requirements. SugarCRM management tracks which employees have attended and completed the annual training **(2.6)**.

SugarCRM has provided information to clients and employees on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by SugarCRM in the event there are problems **(2.7)**. Clients may either contact SugarCRM Support at (877) 842-7276 or visit the Company's contact page on its website at sugarcrm.com/contact. SugarCRM personnel may contact their supervisor to report important matters requiring attention.

Risk Assessment

Risk Management Policies: SugarCRM has documented policies for risk analysis and risk management **(3.1)**. The policies designate responsibility for risk management for SugarCRM as well as outline the process for identifying and addressing risks to the availability, integrity, and confidentiality of data that SugarCRM accesses, stores, and transmits. The risk management policies are made available to all employees through the Company's intranet **(3.2)**.

Risk Assessment: As part of the risk process, SugarCRM management periodically evaluates the risks that may affect SugarCRM's business operations and its ability to maintain the availability, integrity, and confidentiality of data within its system. Internal and external risk assessments are performed annually **(3.3)**. The risk assessments include, but are not limited to, the evaluation of infrastructure, software, people, procedures, and data. A variety of tools are used to perform the risk assessments. The risk assessments include input from SugarCRM personnel from departments throughout SugarCRM, including Business Systems, IT, Security, and members of SugarCRM leadership.

Risks identified from the risk assessments, their ratings, applicable treatment plans, and the status of remedial activities are formally documented **(3.4)**. The internal risk register is updated throughout the year and annually approved to take into consideration relevant changes in SugarCRM's operations and technology environment **(3.5)**.

Monitoring of Controls

Monitoring is a critical aspect of internal control in evaluating whether controls are operating as intended and whether they are modified as appropriate for changing conditions. Management has instituted mechanisms to monitor that any potential problems within the organization are immediately identified and resolved. Management is also responsible for monitoring the quality of the product and services provided to clients. Management regularly engages client personnel to get feedback and determine whether their needs are met in a timely manner.

Internal Monitoring of Controls: SugarCRM's management reviews internal processes supporting the operation of internal controls as well as output from monitoring systems to determine that their controls continue to operate effectively **(4.1)**. If controls are found to be deficient in design or operating effectiveness, the management team puts corrective actions in place. SugarCRM management reviews the SOC audits from their subservice organization to determine whether controls upon which SugarCRM relies are operating effectively **(4.2)**.

Control Activities

SugarCRM has established and implemented policies and procedures to perform periodic assessments and evaluations that consider all elements of security as they apply to AICPA trust services criteria. Findings, recommended actions, and the Company's remediation decisions are communicated to appropriate personnel. SugarCRM conducts both internal and external control assessments to assess the design and operating effectiveness of internal control **(5.1)**. SugarCRM's leadership also meets periodically to review the organization's risks as well as its compliance with critical standards and regulations **(5.2)**. These meetings include management and executive level participation so that knowledge is shared and understood throughout the Company.

Logical and Physical Access

User Access Administration: SugarCRM has developed a process to register and authorize personnel prior to being issued system credentials and granted the ability to access the system **(6.1)**. This process is guided by the principle of least privilege and any access granted must be necessary to perform assigned responsibilities. For new hires, requests for initial IT access, including AWS or administrative access, is originated by the HR department as part of the personnel onboarding process. Access requests or changes are documented in the onboarding IT request ticket and approved by the new hire's manager or HR **(6.2)**. For client access to the SugarCRM platform, SugarCRM will create an administrator account that has the ability to create subsequent user accounts in their specific SugarCRM platform instance.

Complementary User Entity Controls: *User entities are responsible for provisioning access to users on their instance of the SugarCRM platform.*

In addition, there is a process to remove access when an individual terminates employment with SugarCRM. Prior to or on the day of termination, an exit checklist is completed that documents the removal of system access **(6.3)**. As part of the process to complete the offboarding checklist, access to all systems used by SugarCRM is reviewed for accounts assigned to the terminated personnel. As accounts are identified, they are disabled or removed. Terminated personnel's access to SugarCRM's platform and client data is removed within 24 hours of the termination date **(6.4)**.

Complementary User Entity Controls: *User entities are responsible for administering their personnel's access to their instance of the SugarCRM platform, including the removal of users' access to the system.*

Administrator and Remote Access: Access to the production environment at an infrastructure level occurs via the AWS admin console or direct access to the servers via a bastion host. SugarCRM has also created a custom application that mediates access to the production environment. To access the production environment, operations and support personnel must first authenticate to the custom SugarCRM platform via the corporate single sign-on (SSO) solution and the multifactor authentication (MFA) support tool **(6.5)**. Administrator-level access privileges to the production environment are restricted to only those individuals who require such access to perform their respective job functions **(6.6)**. After authentication occurs, admins must enable access through the application, which creates an account that can be used to access the production client environment. Before access is granted, administrators must also enter a support ticket number that substantiates the requirement to access client environments, and access is logged **(6.7)**. Once the reference ticket is entered, then access to client environments—either the client application instance or the infrastructure—is available. Access to the production environment via the bastion hosts use secure shell protocol (SSH), which is configured with strong encryption algorithms; MFA is also required **(6.8)**. Access to the corporate environment is controlled via a virtual private network (VPN). Access to the corporate VPN is limited to authorized individuals, and communications are encrypted using strong encryption algorithms **(6.9)**.

Access to Client Data: Sensitive client data is stored within SugarCRM's production file systems. Access to client data within the SugarCRM platform file systems by SugarCRM employees is restricted to authorized employees **(6.10)**.

Encryption of Client Data: SugarCRM understands the sensitivity of its clients' data and has, therefore, implemented security controls to protect the confidentiality of the data. Client data within the SugarCRM platform production file systems is encrypted **(6.11)**.

Password Management: Infrastructure and application password parameters have been configured to be compliant with the SugarCRM password policy and industry best practices. Access to the AWS admin console requires complex passwords and requires MFA **(6.12)**. Passwords to the domain are required to be complex **(6.13)**. Password parameters for the SugarCRM application are configurable by SugarCRM clients.

Complementary User Entity Controls: *User entities are responsible for implementing password complexity rules and expiration within their instance of SugarCRM that meet their security requirements.*

Complementary User Entity Controls: *User entities are responsible for maintaining security of authentication credentials for their users.*

Workstation Use and Security: The Company's policies and procedures provide guidance to its personnel concerning the physical safeguarding of workstations with access to the IT environment. The guidance is appropriate to the workstation type (e.g., fixed workstation, portable workstation/laptop computer, tablet computer, smartphone, etc.) and location (office, home, public place, etc.). To minimize the risk that data is compromised in the event that hardware or data is lost or stolen, SugarCRM has encrypted workstations using FileVault or BitLocker, as appropriate to the host **(6.14)**.

Complementary User Entity Controls: *User entities are responsible for configuring session timeouts within their instance of SugarCRM.*

Physical Access: SugarCRM no longer has physical office space. Personnel are working remotely indefinitely to support clients and the services. As such, critical physical access controls are those at the hosting facility owned and managed by AWS.

Access Reviews: Management performs an annual security access review that includes reviewing access to the SugarCRM platform, firewalls, and production servers **(6.15)**.

Inventory of Information Assets: SugarCRM maintains an inventory listing of information assets in order to protect them from security events and maintain the confidentiality of data and availability of information **(6.16)**.

Firewalls: Firewalls protecting the SugarCRM network are configured to block unauthorized traffic **(6.17)**. Access to modify firewall rules is restricted to authorized individuals **(6.18)**. Firewall rules are reviewed on an annual basis and updated as necessary **(6.19)**. Inbound network traffic to the hosts in the AWS environment is controlled via the use of security groups **(6.20)**.

Transmission Encryption: All data transfers between users and the SugarCRM platform are secured using TLS and industry-standard encryption **(6.21)**.

Complementary User Entity Controls: *User entities that provide data to SugarCRM are responsible for the security of the data transmission.*

Removable Media: SugarCRM has taken measures to restrict personnel use of removable media to help mitigate both the risk of data loss as well as the risk of malware being introduced onto the SugarCRM platform **(6.22)**.

Hardware and Data Disposal: SugarCRM's policies related to media protection address the handling of devices and media that may potentially contain sensitive Company or client data. SugarCRM defines specific requirements for hardware and data disposal in its security policies. Electronic equipment is wiped of all data or is physically destroyed by a well-known third party who specializes in secure media destruction **(6.23)**.

Client Segregation: Maintaining segregation of access to client SugarCRM platform instances and associated data is critical. Technical implementations are in place so that segregation of access to data exists within SugarCRM client environments. SugarCRM clients are restricted to their own platform instance through the use of unique user IDs (username and password) mapped to their data only **(6.24)**.

System Operations

Incident Response Plan: SugarCRM has a documented incident response plan (IRP) that establishes the procedures to be undertaken in response to information security incidents across the SugarCRM platform **(7.1)**. The policy addresses the phases of incident response to include preparation, identification, containment, eradication, recovery, and lessons learned. It also identifies the members of the incident response team, their associated roles and responsibilities, and communication protocols. The IRP is updated annually, and more frequently, based upon incident outcomes and lessons learned, as appropriate **(7.2)**.

On an annual basis, SugarCRM conducts a test of the IRP and the ability of the Incident Response Team to execute the plan on an annual basis, and documents the test procedures and test results **(7.3)**. Gaps, areas of improvement, and lessons learned are utilized to modify the plan, as needed.

Incident Monitoring and Recordkeeping: SugarCRM maintains a record of security incidents that is used to track investigation details and resolution of security incidents **(7.4)**. The incident records include a unique identifier, a description of the incident and relevant facts (e.g., information that was disclosed), a SIRT assignee, and current status.

Disaster Recovery Plan: SugarCRM has established and implemented a disaster recovery plan to be activated and followed in the event of damage and/or disruption to the SugarCRM platform systems of sufficient magnitude to warrant activation of the plan **(7.5)**. The plan documents the Company's preparations and actions required for recovering essential corporate and IT operations. A backup schedule is maintained to protect sensitive data from loss in the event of a system failure. All production data is backed up. SugarCRM performs a backup of the SugarCRM platform production environments daily and maintains a rolling 30 days of backups **(7.6)**. In the case of backup failures or errors, SugarCRM personnel are notified and restart the backup process manually **(7.7)**. Backups are restored multiple times throughout the year as part of normal operations **(7.8)**.

Antimalware and Patching: SugarCRM deploys antimalware software on all workstations that can access the production environment, and the software monitors the behavior of software executing on the hosts **(7.9)**. SugarCRM applies critical security patches to user workstations when necessary. Patching needs are identified via continuous monitoring agents **(7.10)**. SugarCRM platform production servers are kept up to date on patching, and patching needs are identified via continuous monitoring agents **(7.11)**.

Vulnerability Assessments: SugarCRM continuously executes external vulnerability scans against the SugarCRM platform and infrastructure to identify potential system vulnerabilities **(7.12)**. When vulnerabilities are identified, the SugarCRM technical team prioritizes the identified vulnerabilities, develops a remediation plan, and addresses vulnerabilities in accordance with the defined service-level agreements. SugarCRM scans the custom code base for security flaws within the SugarCRM platform **(7.13)**.

Infrastructure Auditing: SugarCRM audits successful and failed authentication events on firewalls **(7.14)**. Authentication events to the SugarCRM platform production infrastructure are audited **(7.15)**

Audit Reduction, Review, and Analysis: Audit logs must be managed and protected so that they accurately reflect the activities conducted on organizational systems, but if audit logs are not reviewed and analyzed, they will be of little use to an organization to detect an intrusion, actual or attempted. If audit logs are not managed, protected, and analyzed, attackers can erase their tracks, hide more efficiently, and persist their presence in corporate environments. Audit logs (e.g., syslog) from the SugarCRM infrastructure are sent to a centralized logging host. SugarCRM uses automated mechanisms to integrate and correlate audit review and analysis processes to support investigations into potential suspicious or malicious activity **(7.16)**. Audit data is maintained for at least one year.

Infrastructure Monitoring: SugarCRM monitors the production environment so that the stability and availability of the environment is maintained. The SugarCRM platform production environment is monitored using an active monitoring system that alerts upon reaching configured thresholds for CPU and disk utilization, read/write throughput, as well as server up/down status **(7.17)**. This allows for an immediate proactive response to any potential issues with infrastructure resources. Alerts from monitoring tools are sent to the notification system where SugarCRM personnel are notified of system events that need to be addressed **(7.18)**.

Change Management

An effective system development and maintenance process is critical to the integrity of SugarCRM's platform. The SugarCRM platform is a proprietary and in-house developed system where custom changes are often necessary to enhance system functionality. SugarCRM follows defined development policies and procedures for making changes to the platform and the underlying infrastructure used to support the services provided to its clients **(8.1)**. The policies and procedures document the processes followed to perform the different types of changes performed.

Requests for changes can come internally from management or externally from a client. A ticket is created when a change request is made. Management and their teams meet regularly to discuss needed changes. The prioritization of changes is made in these team meetings. Authorization for a change to be developed is given when a change ticket is assigned to an engineer **(8.2)**. The Company uses the change ticket to document the details related to the change, as well as key actions performed during the process. The code repository is used to enforce version control and to document control points within the change management process **(8.3)**.

Once a change has been developed, it is peer reviewed, tested (when possible), and approved for deployment to production **(8.4)**. The name of individuals performing these steps and the date when the steps were completed are documented in the change ticket and pull request. The code repository also performs automated testing of the change before merging a section of code back into the main branch. The change is

assigned to a release, which is reviewed and approved for deployment **(8.5)**. SugarCRM segregates its development, staging, and production environments **(8.6)**.

SugarCRM communicates details of releases for its SugarCRM platform to its clients by posting release notes on its community site **(8.7)**. The links to the latest releases are posted on the home page of the community site. Release notes for those and earlier releases are available for users to review. The site provides a secure platform for users to engage with each other and SugarCRM. All user-generated content is moderated to maintain compliance with applicable privacy and confidentiality requirements, and appropriate security measures are in place to protect the confidentiality and integrity of customer data.

Risk Mitigation

SugarCRM follows a risk management process to identify, assess, and mitigate threats that may prevent the achievement of the Company's service commitments and system requirements **(9.1)**. See the *Risk Assessment* section for SugarCRM's process to identify and assess risks to the organization. Risks identified from the risk assessments, their ratings, applicable treatment plans, and the status of remedial activities are formally documented **(9.2)**.

SugarCRM has established a business continuity and disaster recovery policy to provide governance and direction to personnel when responding to incidents that would threaten the Company's ability to meet its client commitments and availability requirements **(9.3)**. See the *Systems Operations* section of this description for more details regarding incident response to security incidents.

Subservice Providers Monitoring: SugarCRM understands that risks exist when engaging in business relationships and, as a result, considers those risks that could potentially affect the Company's ability to meet its internal and external business objectives.

SugarCRM uses a subservice provider or vendor to assist with elements of maintaining the security and availability of the services it provides. SugarCRM has established guidance and direction pertaining to vendor management which is defined in the vendor management policy **(9.4)**. To effectively manage its vendors, SugarCRM annually completes a vendor risk assessment **(9.5)**. Vendor risks identified during the risk assessment are recorded in SugarCRM's risk register **(9.6)**. SugarCRM follows its standard risk management processes to assess and mitigate vendor related risks.

(The remainder of this page is left blank on purpose.)

Complementary Subservice Organization Controls (CSOC)

SugarCRM's controls related to the SugarCRM platform cover only a portion of the overall internal control for each user entity of the SugarCRM platform. It is not feasible for the applicable trust services criteria related to the SugarCRM platform to be achieved solely by SugarCRM. Therefore, each user entity's internal control must be evaluated in conjunction with SugarCRM's controls and the related tests and results described in Section IV of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization, as described:

	Amazon Web Services (AWS) Complementary Subservice Organization Controls	**Related Control Criteria**
1.	The subservice organization is responsible for providing the physical security controls protecting the production servers from unauthorized access.	CC6.4-CC6.5
2.	The subservice organization is responsible for providing the environmental controls protecting the production servers.	CC7.2-CC7.5
3.	The subservice organization is responsible for maintaining the availability of the hosted environments 24/7/365.	CC7.2-CC7.5
4.	The subservice organization is responsible for managing and resolving incidents and problems reported by SugarCRM in a timely manner.	CC7.2-CC7.5

(The remainder of this page is left blank on purpose.)

Complementary User Entity Controls (CUEC)

The SugarCRM platform provided by SugarCRM for user entities and the controls at SugarCRM cover only a portion of the user entity's overall system of internal control. It is not feasible for the applicable trust services criteria related to the SugarCRM platform to be achieved solely by SugarCRM. Therefore, each user entity's internal control must be evaluated in conjunction with SugarCRM's controls and the related tests and results described in Section IV of this report, taking into account the related complementary user entity controls identified under each control criteria, where applicable. For user entities to rely on the controls reported herein, each user entity must evaluate its own internal control to determine whether the identified complementary user entity controls have been implemented and are operating effectively.

	Complementary User Entity Controls	**Related Control Criteria**
1.	User entities are responsible for provisioning access to users on their instance of the SugarCRM platform.	CC6.2-CC6.3
2.	User entities are responsible for administering their personnel's access to their instance of the SugarCRM platform, including the removal of users' access to the system.	CC6.2-CC6.3
3.	User entities are responsible for implementing password complexity rules and expiration within their instance of SugarCRM that meet their security requirements.	CC6.1, CC6.6
4.	User entities are responsible for maintaining security of authentication credentials for their users.	CC6.1, CC6.6
5.	User entities are responsible for configuring session timeouts within their instance of SugarCRM.	CC6.1, CC6.6
6.	User entities that provide data to SugarCRM are responsible for the security of the data transmission.	CC6.7

(The remainder of this page is left blank on purpose.)

Section IV – Independent Service Auditor's Description of Tests of Controls and Results

Purpose and Objective of the Independent Auditor's Examination

This report on controls placed in operation and tests of operating effectiveness is intended to provide users of the report with information sufficient to obtain an understanding of those aspects of SugarCRM's controls that may be relevant to clients' internal controls. This report, when coupled with an understanding of the internal controls in place at each client, is intended to assist in the assessment of the total internal control surrounding the SugarCRM platform provided by SugarCRM.

Our examination was limited to those controls performed in SugarCRM's Atlanta, Georgia; Cupertino, California; Denver, Colorado; Raleigh, North Carolina; and Munich, Germany offices in support of the SugarCRM platform. It is each stakeholder's responsibility to evaluate this information in relation to the internal controls in place at each client to obtain an overall understanding of the internal controls and assess control risk. The controls provided by clients and SugarCRM must be evaluated together. If effective control activities are not in place at the client, SugarCRM's controls may not compensate for such weaknesses.

Our examination included inquiries of appropriate management, supervisory, and staff personnel; inspection of documents and records; observation of activities and operations; and tests of controls surrounding the Company's SugarCRM platform. Our tests of controls were performed throughout the period March 1, 2023 to February 29, 2024 and were applied to those controls relating to the applicable trust services criteria.

The description of controls is the responsibility of SugarCRM's management. Our responsibility is to express an opinion that the controls are operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control criteria, specified by the AICPA, were achieved during the period March 1, 2023 to February 29, 2024.

Any exceptions noted by Linford & Company LLP regarding the operating effectiveness of the controls identified related to the applicable control criteria or the level of compliance with the controls are presented in this section under the caption, "Results of Testing." Concerns identified herein are not necessarily weaknesses in the total system of internal control at SugarCRM as this determination can only be made after consideration of controls in place at each client. Complementary user entity controls that should be exercised by clients in order to complement the controls of SugarCRM to attain the stated criteria are presented in Section III when considered applicable.

Overview of the Internal Control Environment

Entity-level Controls

Our examination considered the control environment and included inquiry of appropriate management and staff, inspection of documents and records, and observation of activities and operations. Our examination of the tests of operating effectiveness was for the period March 1, 2023 to February 29, 2024 and was applied to those controls relating to the applicable trust services criteria.

The control environment represents the collective effect of various elements in establishing, enhancing, or mitigating the effectiveness of specified controls. In addition to our review of the controls placed into operation, our procedures included tests of the relevant elements of SugarCRM's control environment, including SugarCRM's organizational structure and management control methods.

Our evaluation of the control environment included the following procedures, to the extent necessary:

- ✓ *Inspected* SugarCRM's organizational structure and noted the segregation of functional responsibilities, personnel policies, and other policies and procedures.
- ✓ *Inquired* through discussion with management personnel responsible for developing, monitoring, and enforcing controls.
- ✓ *Observed* personnel in the performance of their assigned duties.

No relevant exceptions were noted in entity-level testing.

* * * * *

The results of these procedures were considered in planning the nature, timing, and extent of evaluation procedures around the operating effectiveness of controls.

Controls Specified by SugarCRM, Testing Procedures, and Results of Tests

The following tables include a description of the control activities, testing procedures performed, and results of tests. SugarCRM Management specified the control activities and the AICPA specified the related control criteria in *Section V – SOC 2 Requirements and Controls*.

Control Activities Relevant to the Security Criteria

Control Environment

Ref	Controls Specified by SugarCRM	Testing Performed by Linford & Company	Results of Testing
1.1	The Board meets quarterly throughout the year to review the organization's products and services provided to clients, business strategy, financial information, and other items that are related to the enterprise as a whole.	For a sample of quarters during the period, noted via *inspection* of the meeting minutes that the Board met quarterly to review the organization's products and services provided to clients, business strategy, financial information, and other items that are related to the enterprise as a whole.	No exceptions noted.
1.2	SugarCRM's expectations for all employees to conduct themselves honestly and ethically are communicated in the Company's code of conduct.	*Inspected* the code of conduct and noted that it was updated during the period and outlined management's expectations for ethical conduct within the organization.	No exceptions noted.
1.3	SugarCRM's organizational structure defines authorities across the Company to facilitate information flow and establish responsibilities.	*Inspected* SugarCRM's detailed organizational chart and noted that the chart clearly defined the department and supervisor of each employee and contractor.	No exceptions noted.

Control Environment (continued)

Ref	Controls Specified by SugarCRM	Testing Performed by Linford & Company	Results of Testing
1.4	To increase the operational effectiveness of employees within this structure, every position has a job description so individuals understand their roles and responsibilities.	For a sample of job titles, *inspected* the job descriptions for the positions and performed *inquiries* of management and noted that the job descriptions existed and correlated with the job role and responsibilities.	No exceptions noted.
1.5	During the resume review and the interview process, technical competence is evaluated for selected candidates by the interviewer.	For a sample of newly hired employees during the period, *inspected* the new hire interview feedback forms and noted that each candidate's technical competence was evaluated during the screening and interview process.	No exceptions noted.
1.6	Applicants for employment at SugarCRM are screened to determine whether past behavior aligns with company policies and procedures.	For a sample of newly hired employees and contractors during the period, *inspected* the completed background checks or screening results (non-U.S.) and noted that a background screening was completed.	No exceptions noted.
1.7	New hires are required to review and sign the SugarCRM employee handbook (U.S. personnel) or the employment agreement (non-U.S. personnel), confidentiality agreement, and security policies to evidence that they will abide by the company policies as outlined in the provided documents.	For a sample of newly hired employees during the period, *inspected* the signed handbooks for U.S. personnel or employment agreements for non-U.S. personnel, confidentiality agreement, and security policies and noted that each individual selected signed the relevant documents to evidence they acknowledged the policies.	No exceptions noted.

Control Environment (continued)

Ref	Controls Specified by SugarCRM	Testing Performed by Linford & Company	Results of Testing
1.8	After the first year of employment, performance reviews occur at least annually.	For a sample of employees, *inspected* completed performance reviews and noted that an annual performance review was performed.	No exceptions noted.
1.9	To assist with SugarCRM's commitments to security, SugarCRM management provides mandatory security awareness training for new hires and annually each year thereafter.	For a sample of newly hired employees during the period, *inspected* the training records and noted that the individual completed the onboarding trainings that covered security awareness. For a sample of employees, *inspected* training records and noted that annual security awareness training was completed during the period.	No exceptions noted. No exceptions noted.
1.10	Consulting agreements with contracting agencies address confidentiality of proprietary and confidential information of SugarCRM.	For a sample of contracting agencies employed by SugarCRM, *inspected* the consulting agreement and noted that the agreement addressed confidentiality.	No exceptions noted.

Information and Communication

Ref	Controls Specified by SugarCRM	Testing Performed by Linford & Company	Results of Testing
2.1	SugarCRM maintains internal documentation that specifies the Company's security policies to communicate certain responsibilities to SugarCRM personnel and system boundaries, which helps them understand their roles within the organization.	Through *inspection* of the SugarCRM repository of policies, noted that SugarCRM maintained policies and procedures to communicate employee roles and responsibilities, and the policies were available to personnel via the Company SharePoint (SugarSource).	No exceptions noted.
2.2	SugarCRM has an organizational reporting structure with defined reporting lines and authority hierarchy that delineates roles and responsibilities.	*Inspected* the organizational chart and noted that reporting lines and authority were delineated in the chart.	No exceptions noted.
2.3	SugarCRM has also created a high-level overview of its SugarCRM platform used to describe the services provided to the clients that the SugarCRM platform serves.	*Inspected* the SugarCRM platform and services overview on the Company's website and noted that high-level platform and service overviews were available to internal and external users.	No exceptions noted.
2.4	SugarCRM and its clients' responsibilities and commitments regarding the acceptable use of the SugarCRM platform are included within the MSA, which clients must agree to before using the SugarCRM platform.	Through *inspection* of SugarCRM's standard MSA, noted that it contained the acceptable use description and responsibilities and commitments for SugarCRM and its clients.	No exceptions noted.

Information and Communication (continued)

Ref	Controls Specified by SugarCRM	Testing Performed by Linford & Company	Results of Testing
2.5	To assist with SugarCRM's commitments to security, SugarCRM management provides annual training for employees that covers information security and data protection.	*Inspected* training records for a sample of employees and noted that each employee selected completed their required annual security training during the period.	No exceptions noted.
2.6	SugarCRM management tracks which employees have attended and completed the annual training.	Through *inspection* of the annual training record retention system, noted that SugarCRM had implemented a mechanism for tracking the completion of the annual training of personnel.	No exceptions noted.
2.7	SugarCRM has provided information to clients and employees on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by SugarCRM in the event there are problems.	Through *inspection* of the 'Contact us' page on the SugarCRM website, noted that several methods for contacting SugarCRM existed for clients to report matters in the event of a problem. Through *inquiries* of management, determined that SugarCRM personnel may contact their supervisor, the general counsel, or the Board in the event of a problem. Additionally, personnel may submit concerns anonymously through the HR system.	No exceptions noted. No exceptions noted.

Risk Assessment

Ref	Controls Specified by SugarCRM	Testing Performed by Linford & Company	Results of Testing
3.1	SugarCRM has documented policies for risk analysis and risk management.	Through *inspection* of the policies, noted that SugarCRM maintained documented risk management policies that included risk analysis and risk management.	No exceptions noted.
3.2	The risk management policies are made available to all employees through the Company's intranet.	*Inspected* the Company's shared drive and ascertained that SugarCRM's risk management policies were available to employees on the Company's intranet.	No exceptions noted.
3.3	Internal and external risk assessments are performed annually.	*Inspected* SugarCRM's internal risk register and noted that the Company had reviewed and approved documented risks during the period. *Inspected* SugarCRM's annual external risk assessment report and determined that a third party had completed an assessment of SugarCRM's risk profile during the period.	No exceptions noted. No exceptions noted.

Risk Assessment (continued)

Ref	Controls Specified by SugarCRM	Testing Performed by Linford & Company	Results of Testing
3.4	Risks identified from the risk assessments, their ratings, applicable treatment plans, and the status of remedial activities are formally documented.	*Inspected* SugarCRM's internal risk register and noted that the register included likelihood, impact, and residual risk ratings. *Inspected* SugarCRM's internal risk register and noted that the register included applicable risk treatment plans and the current status of each action item. *Inspected* Board meeting presentation materials and noted that that the materials included actions items and planned timelines to address recommendations noted in the most recent annual external risk assessment report.	No exceptions noted. No exceptions noted. No exceptions noted.
3.5	The internal risk register is updated throughout the year and annually approved to take into consideration relevant changes in SugarCRM's operations and technology environment.	*Inspected* SugarCRM's internal risk register and noted that it included risks pertaining to SugarCRM's operations and technology environment and it had been approved during the period.	No exceptions noted.

Monitoring of Controls

Ref	Controls Specified by SugarCRM	Testing Performed by Linford & Company	Results of Testing
4.1	SugarCRM's management reviews internal processes supporting the operation of internal controls as well as output from monitoring systems to determine that their controls continue to operate effectively.	*Inspected* the control maturity assessment and noted that the information security team performed a maturity assessment of internal controls and reported results to management during the period.	No exceptions noted.
4.2	SugarCRM management reviews the SOC audits from their subservice organization to determine whether controls upon which SugarCRM relies are operating effectively.	*Inspected* the documented management SOC reviews and noted that SugarCRM management reviewed the SOC report of AWS, their most critical subservice provider.	No exceptions noted.

Control Activities

Ref	Controls Specified by SugarCRM	Testing Performed by Linford & Company	Results of Testing
5.1	SugarCRM conducts both internal and external control assessments to assess the design and operating effectiveness of internal control.	*Inspected* the SugarCRM documented risk assessments and determined that an internal security risk assessment was conducted and documented during the period. Through *inspection* of the assessment, ascertained that SugarCRM contracted with a third party to perform an internal control assessment.	No exceptions noted. No exceptions noted.
5.2	SugarCRM's leadership also meets periodically to review the organization's risks as well as its compliance with critical standards and regulations.	*Inspected* a sample of quarterly risk assessment presentations during the period and noted that leadership reviewed the risk assessment updates to understand SugarCRM's compliance with critical standards and regulations.	No exceptions noted.

Logical and Physical Access

Ref	Controls Specified by SugarCRM	Testing Performed by Linford & Company	Results of Testing
6.1	SugarCRM has developed a process to register and authorize personnel prior to being issued system credentials and granted the ability to access the system.	*Inspected* SugarCRM's access control policy and noted it specified that personnel were only granted access to sensitive data to support a business need.	No exceptions noted.
6.2	Access requests or changes are documented in the onboarding IT request ticket and approved by the new hire's manager or HR.	For a sample of new hires during the period, *inspected* the onboarding IT request and noted that access was approved by the new hire's manager or HR.	No exceptions noted.
6.3	Prior to or on the day of termination, an exit checklist is completed that documents the removal of system access.	For a sample of terminations during the period, *inspected* the termination ticket and noted that it documented tasks completed as part of personnel termination and included removal of logical access to the SugarCRM platform.	No exceptions noted.
6.4	Terminated personnel's access to SugarCRM's platform and client data is removed within 24 hours of the termination date.	For a sample of terminations during the period, *inspected* relevant system active user access listings and noted that access to the SugarCRM platform and client data was removed within 24 hours of the termination date.	No exceptions noted.
6.5	To access the production environment, operations and support personnel must first authenticate to the custom SugarCRM platform via the corporate SSO solution and the MFA support tool.	*Inspected* authentication parameters to the SugarCRM platform production environments and noted that each required authentication via SugarCRM's SSO solution and required MFA.	No exceptions noted.

Logical and Physical Access (continued)

Ref	Controls Specified by SugarCRM	Testing Performed by Linford & Company	Results of Testing
6.6	Administrator-level access privileges to the production environment are restricted to only those individuals who require such access to perform their respective job functions.	*Inspected* all users with administrative access to the production environment and tools, determined the users' job roles via the organizational chart, and noted that the users were current employees and the access granted appeared appropriate per their job role. Further, performed *inquiries* of management and determined that all users' access was appropriate and approved.	No exceptions noted. No exceptions noted.
6.7	Before access is granted, administrators must also enter a support ticket number that substantiates the requirement to access client environments, and access is logged.	*Inspected* login configuration requirements and noted that a support ticket number was required to access client environments via the command line and the custom application that mediated access to the production environment. *Inspected* authentication activity and noted that all access to the production environment was logged.	No exceptions noted. No exceptions noted.
6.8	Access to the production environment via the bastion hosts use SSH, which is configured with strong encryption algorithms; MFA is also required.	*Inspected* the SSH configurations and noted that it was systematically configured to use strong encryption algorithms. *Inspected* the SSH authentication process and noted that MFA was required for access to the bastion hosts.	No exceptions noted. No exceptions noted.

Logical and Physical Access (continued)

Ref	Controls Specified by SugarCRM	Testing Performed by Linford & Company	Results of Testing
6.9	Access to the corporate VPN is limited to authorized individuals, and communications are encrypted using strong encryption algorithms.	*Inspected* a sample of users with access to the corporate VPN and the bastion host, as well as the users' job roles via the organizational chart, and noted that each user was a current employee and the access granted appeared appropriate per their job role. Further, performed *inquiries* of management and determined that the selected users' VPN access was appropriate and approved. *Inspected* encryption algorithms and noted that the VPN was configured to use strong encryption algorithms.	No exceptions noted. No exceptions noted. No exceptions noted.
6.10	Access to client data within the SugarCRM platform file systems by SugarCRM users is restricted to authorized employees.	*Inspected* a sample of users with access to client data within the SugarCRM platform production file systems and determined the users' job roles via the organizational chart and noted that each user was a current employee and the access granted appeared appropriate per their job role. Further, performed *inquiries* of management and determined that the selected users' file systems access was appropriate and approved.	No exceptions noted. No exceptions noted.

Logical and Physical Access (continued)

Ref	Controls Specified by SugarCRM	Testing Performed by Linford & Company	Results of Testing
6.11	Client data within the SugarCRM platform production file systems is encrypted.	*Inspected* encryption configurations and noted that client data in the SugarCRM platform production file systems was encrypted.	No exceptions noted.
6.12	Access to the AWS admin console requires complex passwords and requires MFA.	*Inspected* authentication requirements and noted that access to the AWS admin console and AWS root access required complex passwords and MFA.	No exceptions noted.
6.13	Passwords to the domain are required to be complex.	*Inspected* password parameter settings and noted that passwords for the SugarCRM domain were required to be complex.	No exceptions noted.
6.14	To minimize the risk that data is compromised in the event that hardware or data is lost or stolen, SugarCRM has encrypted workstations using FileVault or BitLocker, as appropriate to the host.	For a sample of workstations, *inspected* encryption settings and noted that encryption was enabled.	No exceptions noted.
6.15	Management performs an annual security access review that includes reviewing access to the SugarCRM platform, firewalls, and production servers.	*Inspected* the annual security access review and noted that a security access review was completed including access to the SugarCRM platform and supporting infrastructure.	No exceptions noted.
6.16	SugarCRM maintains an inventory listing of information assets in order to protect them from security events and maintain the confidentiality of data and availability of information.	*Inspected* the SugarCRM inventory listing and noted that SugarCRM maintained an inventory of information assets.	No exceptions noted.

Logical and Physical Access (continued)

Ref	Controls Specified by SugarCRM	Testing Performed by Linford & Company	Results of Testing
6.17	Firewalls protecting the SugarCRM network are configured to block unauthorized traffic.	*Inspected* the firewall configuration and noted that it was configured to block unauthorized internet traffic.	No exceptions noted.
6.18	Access to modify firewall rules is restricted to authorized individuals.	For a sample of individuals with access to modify the firewall rules, *inspected* the organizational chart and noted that each individual with access was a current employee and the access granted appeared appropriate per their job role. Further, performed *inquiries* of management and determined that the selected individuals' access to modify the firewall rules was appropriate and approved.	No exceptions noted. No exceptions noted.
6.19	Firewall rules are reviewed on an annual basis and updated as necessary.	*Inspected* the annual firewall rules review and noted that a firewall review was performed during the period.	No exceptions noted.
6.20	Inbound network traffic to the hosts in the AWS environment is controlled via the use of security groups.	*Inspected* the AWS accounts' configured security groups and noted that each was configured to filter inbound network traffic to production hosts.	No exceptions noted.
6.21	All data transfers between users and the SugarCRM platform are secured using TLS and industry-standard encryption.	*Inspected* third-party security reports and noted that data transfers between users and the SugarCRM platform used TLS and industry-standard encryption.	No exceptions noted.

Logical and Physical Access (continued)

Ref	Controls Specified by SugarCRM	Testing Performed by Linford & Company	Results of Testing
6.22	SugarCRM has taken measures to restrict personnel use of removable media to help mitigate both the risk of data loss as well as the risk of malware being introduced onto the SugarCRM platform.	*Inspected* the removable media policy and noted that controls were in place to control the use of removable media within the SugarCRM platform.	No exceptions noted.
6.23	Electronic equipment is wiped of all data or is physically destroyed by a well-known third party who specializes in secure media destruction.	*Inspected* the certificate of destruction for electronic equipment that was wiped of all data or was physically destroyed during the period and noted that SugarCRM wiped data from decommissioned electronic equipment and media via a third party for decommissioned electronic equipment.	No exceptions noted.
6.24	SugarCRM clients are restricted to their own platform instance through the use of unique user IDs (username and password) mapped to their data only.	*Inspected* logical segmentation and noted that SugarCRM clients were restricted to their own platform instance through the use of unique user IDs (username and password) mapped to their data only.	No exceptions noted.

System Operations

Ref	Controls Specified by SugarCRM	Testing Performed by Linford & Company	Results of Testing
7.1	SugarCRM has a documented IRP that establishes the procedures to be undertaken in response to information security incidents across the SugarCRM platform.	*Inspected* the IRP and noted that it detailed procedures for incident response and specified roles and responsibilities in the event of a security incident.	No exceptions noted.
7.2	The IRP is updated annually, and more frequently, based upon incident outcomes and lessons learned, as appropriate.	*Inspected* the IRP and determined that it was updated during the period and included lessons learned from the last IRP test.	No exceptions noted.
7.3	On an annual basis, SugarCRM conducts a test of the IRP and the ability of the Incident Response Team to execute the plan on an annual basis, and documents the test procedures and test results.	*Inspected* the annual IRP test and noted that during the period, SugarCRM conducted a tabletop test of its IRP and documented the results and lessons learned.	No exceptions noted.
7.4	SugarCRM maintains a record of security incidents that is used to track investigation details and resolution of security incidents.	*Inspected* the Company's record of security incidents and noted that SugarCRM maintained a log of security incidents during the period. For a sample of security incidents during the period, *inspected* incident resolution tickets and noted that the incidents were tracked through resolution.	No exceptions noted. No exceptions noted.

System Operations (continued)

Ref	Controls Specified by SugarCRM	Testing Performed by Linford & Company	Results of Testing
7.5	SugarCRM has established and implemented a disaster recovery plan to be activated and followed in the event of damage and/or disruption to the SugarCRM platform systems of sufficient magnitude to warrant activation of the plan.	*Inspected* SugarCRM's disaster recovery and business continuity policy and the disaster recovery plan and noted that the documentation was updated during the period and addressed elements of disaster recovery such as backup strategies, testing, and failover.	No exceptions noted.
7.6	SugarCRM performs a backup of the SugarCRM platform production environments daily and maintains a rolling 30 days of backups.	*Inspected* the system backup settings and noted that the SugarCRM platform production environments were backed up nightly and a rolling 30 days of backups were available.	No exceptions noted.
7.7	In the case of backup failures or errors, SugarCRM personnel are notified and restart the backup process manually.	*Inspected* a backup error notification and noted that SugarCRM personnel were notified in the event of backup failures or errors, and resolved the identified issues, as necessary.	No exceptions noted.
7.8	Backups are restored multiple times throughout the year as part of normal operations.	*Inspected* documentation from restorations for each application in the SugarCRM platform and noted that restorations from the backups were performed during the period. Performed corroborative *inquiries* of management and ascertained that backups were restored on a regular basis.	No exceptions noted. No exceptions noted.

System Operations (continued)

Ref	Controls Specified by SugarCRM	Testing Performed by Linford & Company	Results of Testing
7.9	SugarCRM deploys antimalware software on all workstations that can access the production environment, and the software monitors the behavior of software executing on the hosts.	For a sample of workstations, *inspected* workstation configurations and noted that antimalware software was installed and monitored.	No exceptions noted.
7.10	SugarCRM applies critical security patches to user workstations when necessary. Patching needs are identified via continuous monitoring agents.	For a sample of workstations, *inspected* the workstation configurations and noted that the workstations were current on operating system patching and continuously monitored.	No exceptions noted.
7.11	SugarCRM platform production servers are kept up to date on patching, and patching needs are identified via continuous monitoring agents.	For a sample of SugarCRM platform production servers, *inspected* the patch status and noted that the servers were each up to date on patching and continuously monitored in real-time.	No exceptions noted.
7.12	SugarCRM continuously executes external vulnerability scans against the SugarCRM platform and infrastructure to identify potential system vulnerabilities.	*Inspected* the internal and external vulnerability scans executed upon the SugarCRM platform environments and noted that internal and external vulnerability scans were performed.	No exceptions noted.
7.13	SugarCRM scans the custom code base for security flaws within the SugarCRM platform.	*Inspected* the most recent scans generated by the code scanning tools for each application in the SugarCRM platform and noted that the SugarCRM platform code base was scanned for security vulnerabilities and issues identified were remediated.	No exceptions noted.

System Operations (continued)

Ref	Controls Specified by SugarCRM	Testing Performed by Linford & Company	Results of Testing
7.14	SugarCRM audits successful and failed authentication events on firewalls.	*Inspected* firewall logging and noted that successful and failed authentication events on the firewalls were continuously logged and audited, as necessary.	No exceptions noted.
7.15	Authentication events to the SugarCRM platform production infrastructure are audited.	*Inspected* activity logs and noted that authentication events to the SugarCRM platform production infrastructure were audited.	No exceptions noted.
7.16	SugarCRM uses automated mechanisms to integrate and correlate audit review and analysis processes to support investigations into potential suspicious or malicious activity.	*Inspected* the monitoring tool and noted that automated mechanisms were in place to support correlation of audit events and the subsequent review and analysis process.	No exceptions noted.
7.17	The SugarCRM platform production environment is monitored using an active monitoring system that alerts upon reaching configured thresholds for CPU and disk utilization, read/write throughput, as well as server up/down status.	*Inspected* the monitoring tools and noted that the monitoring systems were in place for the SugarCRM platform production environment and the production systems were monitored for CPU and disk utilization, read/write throughput, and server up/down status.	No exceptions noted.
7.18	Alerts from monitoring tools are sent to the notification system where SugarCRM personnel are notified of system events that need to be addressed.	*Inspected* the monitoring tools and notification tool and noted that alerts from monitoring tools were integrated with the notification tool and SugarCRM personnel were alerted via the notification tool of system events related to the SugarCRM platform to be addressed.	No exceptions noted.

Change Management

Ref	Controls Specified by SugarCRM	Testing Performed by Linford & Company	Results of Testing
8.1	SugarCRM follows defined development policies and procedures for making changes to the platform and the underlying infrastructure used to support the services provided to its clients.	*Inspected* the documented change management policies and procedures and noted that SugarCRM documented a defined development process to be followed for changes. Performed *inquiries* of SugarCRM management and ascertained that SugarCRM followed the defined development process for changes to the SugarCRM platform.	No exceptions noted. No exceptions noted.
8.2	Authorization for a change to be developed is given when a change ticket is assigned to an engineer.	For a sample of changes performed during the period, *inspected* the electronic tickets and determined that the changes were each authorized for development.	No exceptions noted.
8.3	The code repository is used to enforce version control and to document control points within the change management process.	*Inspected* the GitHub code repository tool and noted that it was configured to manage version control and record the activities within the change management process. For a sample of changes performed during the period, *inspected* the GitHub code repository tool and determined that it managed version control and recorded peer review and automated testing activities for the changes selected to the SugarCRM platform.	No exceptions noted. No exceptions noted.

Change Management (continued)

Ref	Controls Specified by SugarCRM	Testing Performed by Linford & Company	Results of Testing
8.4	Once a change has been developed, it is peer reviewed, tested (when possible), and approved for deployment to production.	For a sample of changes performed during the period, *inspected* the associated pull requests and noted that the changes were peer reviewed, tested, and approved to be deployed to production.	No exceptions noted.
8.5	The change is assigned to a release, which is reviewed and approved for deployment.	For a sample of releases performed during the period, *inspected* the documented release checklists and determined that the releases were each reviewed and approved.	No exceptions noted.
8.6	SugarCRM segregates its development, staging, and production environments.	*Inspected* SugarCRM's cloud infrastructure and noted that separate development, staging, and production environments were maintained by SugarCRM.	No exceptions noted.
8.7	SugarCRM communicates details of releases for its SugarCRM platform to its clients by posting release notes on its community site.	For a sample of releases performed during the period, *inspected* SugarCRM's support website and determined that release notes were prepared and available for users of the system for each release selected.	No exceptions noted.

Risk Mitigation

Ref	Controls Specified by SugarCRM	Testing Performed by Linford & Company	Results of Testing
9.1	SugarCRM follows a risk management process to identify, assess, and mitigate threats that may prevent the achievement of the Company's service commitments and system requirements.	Through *inspection* of the risk assessment policy and risk register, noted that the Company followed a defined risk management process to identify, assess, and mitigate threats to SugarCRM's ability to meet its service commitments and system requirements.	No exceptions noted.
9.2	Risks identified from the risk assessments, their ratings, applicable treatment plans, and the status of remedial activities are formally documented.	*Inspected* SugarCRM's internal risk register and noted that the register included likelihood, impact, and residual risk ratings. *Inspected* SugarCRM's internal risk register and noted that the register included applicable risk treatment plans and the current status of each action item. *Inspected* Board meeting presentation materials and noted that that the materials included actions items and planned timelines to address recommendations noted in the most recent annual external risk assessment report.	No exceptions noted. No exceptions noted. No exceptions noted.
9.3	SugarCRM has established a business continuity and disaster recovery policy to provide governance and direction to personnel when responding to incidents that would threaten the Company's ability to meet its client commitments and availability requirements.	*Inspected* SugarCRM's business continuity and disaster recovery policy and noted that it defined roles and responsibilities, planning, testing, and compliance requirements for the Company's business continuity and disaster recovery goals and objectives.	No exceptions noted.

Risk Mitigation (continued)

Ref	Controls Specified by SugarCRM	Testing Performed by Linford & Company	Results of Testing
9.4	SugarCRM has established guidance and direction pertaining to vendor management which is defined in the vendor management policy.	*Inspected* the vendor management policy and determined that SugarCRM had established a policy to provide guidance and direction to personnel regarding approved vendor management activities.	No exceptions noted.
9.5	To effectively manage its vendors, SugarCRM annually completes a vendor risk assessment.	*Inspected* SugarCRM's annual assessment of its cloud infrastructure subservice provider and noted that noted that the review was performed during the period and included a review of the subservice provider's third-party attestations.	No exceptions noted.
9.6	Vendor risks identified during the risk assessment are recorded in SugarCRM's risk register.	*Inquired* of management and ascertained that any vendor related risks were recorded in the Company's risk register. *Inspected* SugarCRM's internal risk register and noted that it included risks pertaining to vendors.	No exceptions noted. No exceptions noted.

Section V – SOC 2 Requirements and Controls

The SugarCRM management team is responsible for establishing and maintaining effective controls over its SugarCRM platform. The controls are designed to provide reasonable assurance to SugarCRM management that the following SOC 2 security control criteria are achieved.

In the table that follows, the columns have the following meaning:

SOC 2 Criteria – This column contains, for each criterion evaluated, the reference citation. Each criterion sources from a requirement of the trust services criteria.

Requirement(s) – This column contains the text of the criterion (requirement) directly from the trust services criteria.

Reference – This column contains the reference to the control activities in *Section III – SugarCRM's Description of Its SugarCRM Platform*, which are relevant to the achievement of the criterion.

The purpose of this table is to demonstrate that all SOC 2 control criteria in scope were assessed and that the control activities described in *Section III – SugarCRM's Description of Its SugarCRM Platform*, address the SOC 2 control criteria.

Many of the criteria used to evaluate a system are shared amongst all the criteria. For example, the criteria related to risk management apply to the security, availability, processing integrity, confidentiality, and privacy criteria. As a result, the criteria for the security, availability, processing integrity, confidentiality, and privacy criteria are organized into (a) the criteria that are applicable to all five criteria (common criteria) and (b) criteria applicable only to a single criterion. The common criteria (CC1.0 through CC9.0 in the table that follows) constitute the complete set of criteria for the security trust services criteria as well as the criteria common to the availability, processing integrity, confidentiality, and privacy criteria.

Common Criteria/Security Criteria

Security. The trust services criteria relevant to security address the need for information and systems to be protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the service organization's ability to achieve its service commitments and system requirements.

Security refers to the protection of:

i. information during its collection or creation, use, processing, transmission, and storage, and
ii. systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft, or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

CC1.0 Common Criteria Related to Control Environment

SOC 2 Criteria	Requirement(s)	Reference
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	1.2, 1.6
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	1.1
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	1.3-1.4, 2.1-2.2, 2.4

CC1.0 Common Criteria Related to Control Environment (continued)

SOC 2 Criteria	Requirement(s)	Reference
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	1.5-1.10, 2.5-2.6
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	1.7-1.8, 2.5-2.6

CC2.0 Common Criteria Related to Information and Communication

SOC 2 Criteria	Requirement(s)	Reference
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	2.1-2.7, 3.1-3.4, 4.1-4.2, 5.2, 7.16
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.	1.3-1.4, 2.1-2.6, 7.18
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	2.3-2.4, 2.7, 8.7

CC3.0 Common Criteria Related to Risk Assessment

SOC 2 Criteria	Requirement(s)	Reference
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	3.1-3.5, 9.1-9.2
CC3.2	The entity designs, develops, implements, and operates controls, including policies and procedures, to implement its risk mitigation strategy; reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities; and updates the controls, as necessary.	3.1-3.5, 4.2, 5.2, 7.1-7.2
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	3.3, 5.2
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	3.3-3.5, 9.2-9.3

CC4.0 Common Criteria Related to Monitoring Activities

SOC 2 Criteria	Requirement(s)	Reference
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.	4.1-4.2, 5.1, 6.15, 7.16-7.18
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.	3.3-3.5, 4.1-4.2, 5.1-5.2, 7.12-7.18

CC5.0 Common Criteria Related to Control Activities

SOC 2 Criteria	Requirement(s)	Reference
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.	1.1-9.6
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	1.1-9.6
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.	1.1-9.6

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

SOC 2 Criteria	Requirement(s)	Reference
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.	6.1-6.24
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.	6.1-6.10
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.	6.1-6.10

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

SOC 2 Criteria	Requirement(s)	Reference
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	AWS CSOC
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.	6.11, 6.14, 6.16, 6.22-6.24, AWS CSOC
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	6.12-6.13, 6.17-6.20, 7.9-7.18
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.	6.8-6.9, 6.21
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.	7.9-7.18

CC7.0 Common Criteria Related to System Operations

SOC 2 Criteria	Requirement(s)	Reference
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.	4.1-4.2, 7.9-7.18
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.	4.1-4.2, 7.1-7.18, AWS CSOC
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.	4.1-4.2, 5.1-5.2, 7.1-7.5, AWS CSOC
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.	7.1-7.5, AWS CSOC
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	7.1-7.9, AWS CSOC

CC8.0 Common Criteria Related to Change Management

SOC 2 Criteria	Requirement(s)	Reference
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.	8.1-8.7

CC9.0 Common Criteria Related to Risk Mitigation

SOC 2 Criteria	Requirement(s)	Reference
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	3.1, 7.1-7.9, 9.1-9.3
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	9.4-9.6