System and Organization Controls (SOC2) Type 2

Salesforce Services

Report on Management's Description of Salesforce, Inc.'s Salesforce Services' Covered Services System on the Suitability of the Design and Operating Effectiveness of Controls Relevant to Security, Availability, and Confidentiality

For the Period May 1, 2022 to October 31, 2022

Table of Contents

Section I: Salesforce, Inc.’s Management Assertion

Salesforce, Inc.'s Management Assertion

We have prepared the accompanying Report on Management's Description of Salesforce, Inc.'s Salesforce Services' Covered Services System on the Suitability of the Design and Operating Effectiveness of Controls Relevant to Security, Availability, and Confidentiality for the Period May 1, 2022 to October 31, 2022 (Description) of Salesforce, Inc. (Service Organization) in accordance with the criteria for a description of a service organization's system set forth in the Description Criteria DC section 200 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report (Description Criteria). The Description is intended to provide report users with information about the Salesforce Services' Covered Services system (System) that may be useful when assessing the risks arising from interactions with the System throughout the period May 1, 2022 to October 31, 2022, particularly information about system controls that the Service Organization has designed, implemented and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria for security, availability, and confidentiality set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (applicable trust services criteria).

Salesforce, Inc. uses the Component and Non-affiliated subservice organizations (collectively, Subservice Organizations) specified in Section III to provide the specified functions. The Description includes only the controls of Salesforce, Inc.'s Salesforce Services' Covered Services and excludes controls of the Subservice Organizations. The Description also indicates that certain trust services criteria specified therein can be met only if complementary Subservice Organization's controls assumed in the design of Salesforce. Inc.'s Salesforce Services' Covered Services controls are suitably designed and operating effectively along with the related controls at the Service Organization. The Description does not extend to controls of the Subservice Organizations.

Management of Salesforce, Inc. has prepared a separate description of the services used by the System, which includes the aforementioned complementary Component Subservice Organization controls. This Description should be read in conjunction with the separate Component Subservice Organization SOC reports.

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

a. The Description presents the System that was designed and implemented throughout the period May 1, 2022 to October 31, 2022 in accordance with the Description Criteria.

b. The controls stated in the Description were suitably designed to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated as described and if the Subservice Organizations applied the controls assumed in the design of Salesforce, Inc.'s controls throughout the period May 1, 2022 to October 31, 2022.

c. The Salesforce, Inc. controls stated in the Description operated effectively throughout the period May 1, 2022 to October 31, 2022 to achieve the service commitments and system requirements based on the applicable trust services criteria, if the Subservice Organizations applied the controls assumed in the design of Salesforce, Inc.'s controls throughout the period May 1, 2022 to October 31, 2022.

Salesforce, Inc.

Section II: Independent Service Auditor's Assurance Report

Ernst & Young LLP
Suite 1600
560 Mission Street
San Francisco, CA 94105-2907

Tel: +1 415 894 8000
Fax: +1 415 894 8099
ey.com

Independent Service Auditor's Assurance Report

To the Board of Directors of Salesforce, Inc.:

Scope

We have examined Salesforce, Inc.'s accompanying Report on Management's Description of Salesforce, Inc.'s Salesforce Services' Covered Services System on the Suitability of the Design and Operating Effectiveness of Controls Relevant to Security, Availability, and Confidentiality For the Period May 1, 2022 to October 31, 2022 (Description) of its Salesforce Services' Covered Services system (System) in accordance with the criteria for a description of a service organization's system set forth in the Description Criteria DC section 200 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report (Description Criteria) and the suitability of the design and operating effectiveness of controls included in the Description throughout the period May 1, 2022 to October 31, 2022 to provide reasonable assurance that the service commitments and system requirements were achieved based on the trust services criteria for security, availability, and confidentiality set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (applicable trust services criteria).

Carved-out Component Subservice Organizations: The Salesforce Services' Covered Services system uses Salesforce Corporate Services Covered Services and Heroku Services Covered Services (collectively, Component Subservice Organizations), components of Salesforce, Inc. to perform the functions as specified in Section III. The Description includes only controls of the Salesforce Services' Covered Services system and excludes the controls of the Component Subservice Organizations. Certain controls specified by Salesforce, Inc. can be achieved only if complementary subservice organization controls are suitably designed and operating effectively. The Description identifies the types of complementary controls of the Component Subservice Organizations that are necessary to achieve certain Salesforce Services' Covered Services' service commitments and system requirements. The scope of this examination did not include the complementary controls of the Component Subservice Organizations.

Management of Salesforce, Inc. has prepared a separate description of the services used by the System, which includes the aforementioned complementary Component Subservice Organization controls. This report should be read in conjunction with the separate Component Subservice Organization SOC reports.

Carved-out Non-affiliated Subservice Organization: Salesforce, Inc. uses Amazon Web Services (AWS) (Non-affiliated Subservice Organization) identified in Section III to provide the specified functions. The Description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Salesforce, Inc., to achieve Salesforce, Inc.'s service commitments and system requirements based on the applicable trust services criteria. The Description presents Salesforce, Inc.'s system; its controls; and the types of complementary subservice organization controls that the service organization assumes have been implemented, suitably designed, and operating effectively at AWS.

Our examination did not extend to the services provided by AWS and we have not evaluated whether the controls management assumes have been implemented at AWS have been implemented or whether such controls were suitably designed and operating effectively throughout the period May 1, 2022 to October 31, 2022.

Building a better working world

The information in the accompanying Section V – Other Information Presented by Salesforce, Inc. is presented by management of Salesforce, Inc. to provide additional information and is not part of Salesforce, Inc.'s Description. Such information has not been subjected to the procedures applied in our examination and, accordingly we express no opinion on it.

Salesforce, Inc.'s responsibilities

Salesforce, Inc. 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 the service commitments and system requirements were achieved. Salesforce, Inc. has provided the accompanying assertion titled, Salesforce, Inc.'s Management Assertion (Assertion) about the presentation of the Description based on the Description Criteria and suitability of the design and operating effectiveness of the controls described therein to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria. Salesforce, Inc. is responsible for (1) preparing the Description and Assertion; (2) the completeness, accuracy, and method of presentation of the Description and Assertion; (3) providing the services covered by the Description; (4) identifying the risks that would threaten the achievement of the service organization's service commitments and system requirements; and (5) designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve its service commitments and system requirements.

Service auditor's responsibilities

Our responsibility is to express an opinion on the presentation of the Description and on the suitability of the design and operating effectiveness of the controls described therein to achieve the Service Organization's service commitments and system requirements, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants ("AICPA"). Our examination was also conducted in accordance with the International Standards on Assurance Engagement 3000 (ISAE 3000), Assurance Engagements Other than Audits or Review of Historical Financial Information, issue by the International Auditing and Assurance Standards Board (IAASB). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the Description is presented in accordance with the Description Criteria, and (2) the controls described therein are suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved based on the applicable trust services criteria. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- obtaining an understanding of the system and the service organization's service commitments and system requirements.

- performing procedures to obtain evidence about whether the controls stated in the Description are 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.
- assessing the risks that the Description is not presented in accordance with the Description Criteria and that the controls were not suitably designed or operating effectively based on the applicable trust services criteria.
- testing the operating effectiveness of those controls 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.

We are required to be independent of Salesforce, Inc. and to meet our other ethical responsibilities, as applicable for examination engagements set forth in the Preface: Applicable to All Members and Part 1 – Members in Public Practice of the Code of Professional Conduct established by the AICPA and have applied the AICPA's Statement on Quality Control Standards.

Inherent limitations

The Description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to its own particular needs.

Because of their nature, controls at a service organization 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 evaluation of the fairness of the presentation of the Description, or conclusions about the suitability of the design or operating effectiveness of the controls based on the applicable trust services criteria is subject to the risk that the system may change or that controls at a service organization may become ineffective.

Description of tests of controls

The specific controls we tested and the nature, timing, and results of those tests are listed in the accompanying Section IV – Salesforce, Inc.'s Criteria, Related Controls, and EY's Test Procedures and Results (Description of Tests and Results).

Opinion

In our opinion, in all material respects:

a. The Description presents the Salesforce Services' Covered Services system that was designed and implemented throughout the period May 1, 2022 to October 31, 2022 in accordance with the Description Criteria.

Building a better working world

b. The controls stated in the Description were suitably designed to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria if the controls operated effectively and if the Component and Non-affiliated Subservice Organizations (collectively, Subservice Organizations) applied the controls assumed in the design of Salesforce, Inc.'s controls throughout the period May 1, 2022 to October 31, 2022.

c. The controls stated in the Description operated effectively to provide reasonable assurance that the service commitments and system requirements were achieved based on the applicable trust services criteria throughout the period May 1, 2022 to October 31, 2022, if the Subservice Organization controls assumed in the design of Salesforce, Inc.'s controls operated effectively throughout the period May 1, 2022 to October 31, 2022.

Restricted use

This report, including the description of tests of controls and results thereof in the Description of Tests and Results, is intended solely for the information and use of Salesforce, Inc., user entities of Salesforce, Inc.'s Salesforce Services' Covered Services system during some or all of the period May 1, 2022 to October 31, 2022, and prospective user entities, independent auditors and practitioners providing services to such user entities 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, subservice organizations, or other parties, including complementary Subservice Organization controls assumed in the design of the service organization's controls
- Internal control and its limitations
- User entity responsibilities and how they interact with related controls at the service organization
- 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.

Ernst & Young LLP

December 19, 2022

Section III: Report on Management's Description of Salesforce, Inc.'s Salesforce Services Covered Services System on the Suitability of the Design and Operating Effectiveness of Controls Relevant to Security, Availability, and Confidentiality For the Period May 1, 2022 to October 31, 2022

Overview of Operations

Salesforce, Inc. (Salesforce or the Company), headquartered in San Francisco, California, is an enterprise cloud computing company that provides an integrated customer relationship management platform through various products and services. These products and services (Services) include solutions for enhancing customer success through sales, service, marketing, commerce, engagement, integration, analytics, enablement, and productivity, among others.

Salesforce is committed to achieving and maintaining the trust of its customers. Integral to this mission is providing a security and privacy program that considers data protection matters across the suite of Services, including data submitted by customers to the Services.

The scope of this report includes the Services that host "Customer Data" (as defined within the Main Services Agreement (MSA), which is available from the publicly facing website: https://www.salesforce.com/content/dam/web/en_us/www/documents/legal/salesforce_MSA.pdf) and the software described in the table below (collectively and for purposes of this document only, Salesforce Services' Covered Services system or Covered Services).

Salesforce provides services to companies of all sizes via a multi-tenant cloud-based solution. The solution is a collection of application development, deployment, and hosting services. These services allow customers the ability to purchase, use, and customize Salesforce-deployed applications or use platform capabilities to develop their own applications. With a multi-tenant platform, each organization that uses the application uses a set of shared resources. Organizations share a common codebase and their applications can be customized for their specific needs.

Customers can store data and documents, integrate their services with other applications, perform their own reporting, analytics, and scale up or down with high availability and security.

Salesforce Corporate Services Controls

This report should be reviewed in conjunction with the Salesforce Corporate Services report for details regarding the domains where the Salesforce Services' Covered Services system relies on corporate controls and processes. Salesforce Corporate Services teams are responsible for all or a portion of the following domains:

- Salesforce Board of Directors
- Hiring Practices and Staff Development
- Security Awareness and Training
- Risk Management
- Monitoring of Internal Controls
- Physical Security
- Environmental Safeguards
- Vendor Audit Program

- Logical Security
- Corporate IT Network Architecture and Management
- Endpoint Protection
- Product Security
- Threat and Vulnerability Management
- Security Monitoring
- Incident Management
- Contingency Planning and Business Continuity

The above domains are covered as part of the Salesforce Corporate Services SOC report, which covers common controls, services and oversight across Services offered by Salesforce.

Principal Service Commitments and System Requirements

Salesforce leverages advanced technologies along with the administrative, technical, and physical controls to ensure the security, confidentiality, and availability of the Salesforce Services' Covered Services system. Salesforce's Trust and Compliance commitments to customers are communicated via MSA, the Service Level Agreements (SLA) detailed in the MSAs and the online Security, Privacy, and Architecture (SPARC) documentation. Together these documents define the broad set of Trust and Compliance commitments, including, but not limited to:

- Service availability
- Architecture and data segregation
- Security controls
- Security policies and standards
- Security logging
- Incident management
- User authentication
- Physical security
- Reliability and backup
- Disaster recovery
- Data encryption
- Deletion of Customer Data

The Salesforce Services and B2B Commerce SPARC documents are managed and updated by the Legal organization, with input and collaboration from relevant stakeholders. The Salesforce Services and B2B Commerce SPARC documents are reviewed and updated at least annually and as needed. The Trust and Compliance commitments for the Salesforce Services' Covered Services system that form the basis for the description of the controls herein are defined in the Salesforce Services and B2B Commerce SPARC documents published August 26, 2022.

Description of Covered Services

Salesforce Services is responsible for components of infrastructure (i.e., software that comprise the Salesforce Services Covered Services system infrastructure), data security, data storage, and service management processes (i.e., the operation and management of the infrastructure, system, and software engineering life cycles).

This report covers the general information system controls related to the Salesforce Services Covered Services system described below:

Service Name	Service Description
Sales Cloud	Sales Cloud is a cloud-based application designed to help salespeople sell more effectively by centralizing customer information, logging interactions with the company, and automating many of the tasks salespeople do every day. Sales Cloud enables collaboration across a global organization, including social intelligence (e.g., Twitter, LinkedIn), and supports secure sharing and publishing of files, including search capabilities.
Service Cloud	Salesforce's enterprise CRM application for customer service, Service Cloud allows customers to provide customized support to their customers and manage customer accounts, cases, and interactions via email, and chat. Service Cloud applications can be fully integrated with a company's call-center telephony and back-office applications. Service Cloud has many features that are included within the scope of this report including, but not limited to, the live chat feature Chat (formerly Live Agent), Salesforce Scheduler, Salesforce Surveys, and Einstein Next Best Action. **Salesforce Surveys** Salesforce Surveys is a survey tool built natively on the Salesforce Platform. Customers can collaborate to create easy-to-use surveys for collecting actionable insights and feedback. The survey creators can build their own surveys, send them to customers, or embed them in community pages. Results of the survey are stored in the creators' org, so they can harness the power of Salesforce to view data, create reports and dashboards, and share insight.

Service Name	Service Description
Service Cloud (continued)	**Einstein Next Best Action** Display the recommendations to customers at the right time with Einstein Next Best Action. Create and display offers and actions for users that are tailored to meet unique criteria. Develop a strategy that applies business logic to refine those recommendations. Customer strategy distills recommendations into a few key suggestions, like a repair, a discount, or an add-on service. Display the final recommendations in the Lightning app or community.
Salesforce Mobile App (iOS/Android)	The Salesforce app is Salesforce on a mobile device. This enterprise-class mobile experience gives users real-time access to the same information users see on their desktop, but in a convenient mobile experience.
Experience Cloud (formerly branded as Community Cloud)	Salesforce Experience Clouds are branded spaces where user employees, customers, and partners can share information and collaborate. Users can customize and create communities to meet their business needs, then transition seamlessly between them. Multiple communities can be created within the user organization for different purposes.
Chatter	Chatter extends the platform capabilities by offering users real-time enterprise collaboration and communication capabilities. Chatter allows users to instantly interact through profiles, groups, status updates, feeds, content sharing, and app updates. With Chatter, users can also share documents securely and engage each other socially. Chatter is private for the user's instance of Salesforce, and any content in Chatter is only shared with users of that organization. The role-based sharing model and user permissions implemented for the user's instance of the platform apply to Chatter. Users and administrators use the same web interface to access application functionality, but the security controls reside at the platform level.
Lightning Platform (including Force.com and Salesforce Connect)	The Lightning Platform, which excludes Lightning Platform Developer Edition and its associated products and services that are provided for free, is a Platform as a Service (PaaS) delivery model that allows customers to develop custom applications and sites using predefined programming languages and by customizing Salesforce developed application templates and system objects. The Lightning Platform enables developers to customize and deploy business applications entirely on-demand by developing custom code (e.g., using Apex). The platform also includes easy-to-use, point-and-click customization tools to help customers without any programming experience create solutions for unique business requirements. The Covered Services also include Salesforce Connect, which is a feature of Lightning Platform. It provides seamless integration of data across system boundaries by letting users view, search, and modify data that's stored outside of the customer's org.

Service Name	Service Description
Site.com	The Site.com platform supports the creation of sites that can be published as a corporate, social mobile, and micro site. Business users can edit their own content and add or modify content by using 'drag and drop' features. These changes to the site do not require a planned downtime.
Database.com	The Database.com platform is a stripped-down Salesforce Platform that provides a low-cost option for development in the cloud. It has a rich set of Application Program Interfaces (API) that can be accessed from modern frameworks, languages, or devices. Customers can query their data from an application or establish a secure stream of updates to a mobile device.
CRM Analytics (formerly branded as Tableau CRM) (including Einstein Discovery and Salesforce Data Pipelines)	CRM Analytics, which includes Einstein Discovery and Salesforce Data Pipelines, allows customers to connect data from multiple sources and create interactive views and dashboards to share. CRM Analytics datasets can contain Salesforce data, external data, or a combination. Salesforce data can be integrated using a dataflow, which is a reusable set of instructions that defines how to extract data from Salesforce and load it into datasets. CRM Analytics provides customers with the ability to connect Salesforce data or external data and create custom views of datasets and dashboards. By viewing, exploring, refining, saving, and sharing datasets and dashboards, customers can use CRM Analytics dashboards to ultimately support data-based decisions by presenting data in a visually tangible manner. **Einstein Discovery** Einstein Discovery is a Salesforce business machine learning platform that learns patterns from historical data which can be used to predict future outcomes. Customers with domain knowledge of their business can build and deploy predictive models code-free. **Salesforce Data Pipelines** Salesforce Data Pipelines provide fast and scalable data processing and extract, transform, load (ETL) for the customer Salesforce org, supporting external data and machine learning powered data transformation.
IoT Explorer	IoT Explorer allows customer IoT strategies to integrate into the Salesforce Platform, giving business strategists the opportunity to start exploring and implementing their IoT solutions with out-of-the-box access to all their Salesforce data.

Service Name	Service Description
Salesforce Shield	Salesforce Shield is a product offering built on the Salesforce Platform and provides customers a means to protect their enterprise with point-and-click tools that enhance trust, transparency, compliance, and governance across their business-critical apps. **Salesforce Platform Encryption** Platform Encryption allows users to natively encrypt their most sensitive data at rest across their Salesforce apps. Platform Encryption is designed to allow users to retain critical app functionality – like search, workflow, and validation rules – so users maintain full control over encryption keys and can set encrypted data permissions to protect sensitive data from unauthorized users. **Salesforce Event Monitoring** Customers can gain access to detailed performance, security, and usage data on Salesforce apps. Every interaction is tracked and accessible via APIs, so users can view it in the data visualization app of their choice. See who is accessing critical business data, when, and from where. Understand user adoption across apps. Troubleshoot and optimize performance to improve end-user experience. Event Monitoring data can be easily imported into any data visualization or application monitoring tool, such as Einstein Analytics, Splunk, or FairWarning. **Salesforce Field Audit Trail** Whether for regulatory compliance, internal governance, audit, or customer service, Field Audit Trail lets users know the state and value of their data for any date, at any time. Built on a big data backend for massive scalability, Field Audit Trail helps companies create a forensic data-level audit trail, and sets triggers for when data is deleted.
WDC	WDC is a suite of sales-management and service-management tools that help managers and teams learn faster and perform better. WDC has various features to help sales and service teams. This includes recognition tied to real rewards, detailed goals and real-time coaching, and full-featured performance reviews. Since WDC is built on the same underlying Salesforce infrastructure as the Lightning Platform, from an end user perspective WDC inherits many of the same security features and configurable security options as the platform. However, profiles and permissions sets must be configured for WDC features.

Service Name	Service Description
Industry Clouds	The Salesforce Industry Clouds are built on the Salesforce Platform. The Industry Clouds allow enterprises to streamline workflow, increase productivity, deliver more targeted service, and drive deeper customer engagement. The industry-specific applications are mobile friendly and interoperable with other of Salesforce's Services, helping to tailor products that meet the unique needs of specific industries. The scope for the Industry Cloud Platform covers the solutions mentioned below: **Health Cloud** Health Cloud is designed to support the healthcare and life sciences (HLS) industries, including healthcare providers, payers, and pharma and med tech companies, and to help enable HLS organizations to better serve their patients, plan members, customers, and stakeholders. Health Cloud allows HLS organizations to gain a more complete view of their patients and plan members by allowing integration of information from multiple sources, such as electronic health records, medical devices, and wearables and keep track of information such as household information and social determinants of health. Health Cloud also helps HLS organizations to engage more efficiently with patients by offering functionality to define and automate processes, including patient enrollment and intake, referrals and prior authorizations, consent management and care management. In addition, HLS organizations in the pharma and med tech sectors can use Health Cloud to help manage their sales and supply needs for the products and devices they offer to their end customers. **Financial Services Cloud** Financial Services Cloud is designed to support the financial services industry, including wealth management, retail banking, commercial bank and insurance carrier markets, and enable the financial institutions to better serve their clients. Financial Services Cloud allows for managing, updating, and displaying customer data; facilitating engagement with financial institution clients; and managing relationships between the financial institution and clients, as well as offers functionality to define processes in order to automate the preceding. **Manufacturing Cloud** Manufacturing Cloud delivers a new level of business visibility and collaboration between the sales and operations organizations of a manufacturing company. This allows them to have a better view of their customers through powerful new sales agreements and account-based forecasting solutions, providing visibility into their customer interactions while enabling them to generate more robust sales forecasts.

Service Name	Service Description
Industry Clouds (continued)	**Public Sector Solutions** Public Sector Solutions are pre-built applications and purpose-built tools designed to help public sector organizations serve and grow thriving communities. These solutions are most helpful for agencies and government contractors looking to rapidly deploy a future-proof, scalable platform to modernize constituent and employee services. Deliver customer-centric, fast, and seamless experiences at scale.
Salesforce Configure Price Quote (CPQ) and Salesforce Billing (together formerly branded as Quote to Cash (QTC))	Salesforce CPQ and Salesforce Billing are built on the Sales Cloud platform. In addition, there are related packages that add functionality and/or integrations with other systems. These packages include, but are not limited to, advanced approvals, payment gateway integrations, document generation integrations, tax engine integrations, etc. **Salesforce Configure Price Quote (CPQ)** CPQ extends the standard features of Sales or Service Cloud to easily find the right products and services with guided selling; handle complex configurations with bundles and nested configuration; manage subscriptions, contracted pricing, and discount approvals; generate contracts and proposals; and create orders from completed quotes. **Salesforce Billing** Billing automates and speeds up the billing and collection process with features that let users rate usage consumption, automatically apply taxes, easily process invoices and automate payment collection, and report revenue recognition.
B2B Commerce (formerly branded as CloudCraze) and B2B Commerce on Lightning Experience	Salesforce B2B Commerce is built natively on Salesforce and sold into existing Sales, Service, and Experience Cloud customers. For Salesforce customers who want to grow their business by selling products online, it gives them the ability to provide their customers with the seamless, self-service experience of online shopping with all the B2B functionality they demand to grow sales, reduce the cost to serve, and deploy fast.
Salesforce Private Connect	Salesforce Private Connect enables customers to establish private communications between Salesforce and AWS. Salesforce Private Connect establishes the connection without exposing sensitive data traffic to the public internet, manages the end-to-end connections and streamlines access controls.

Service Name	Service Description
Salesforce.org	Salesforce.org is a social impact center focused on partnering with the global community to tackle the world's biggest problems. Salesforce.org builds powerful technology for, and with, its community of nonprofits, schools, and philanthropic organizations. With their guidance, the services help entities operate effectively, raise funds, and connect. The scope of the Salesforce.org products included in the Covered Services is below: **Nonprofit Success Pack (NPSP)** Nonprofit Success Pack (NPSP) is an open source app offered to existing Salesforce Enterprise Licensed customers offering tools to manage programs, donations, volunteers, and supporters – all in one place. It allows customers to streamline fundraising processes and manage missions in real-time with pre-configured but customizable reports and dashboards. Key features of NPSP include: • Constituent and Donor Management • Donation and Grant Management • Engagement Management • Volunteer Management • Reporting and Analytics • Mobile, Social, and Cloud **Program Management Module (PMM)** Program Management Module (PMM) provides a standard framework for nonprofits to get up and running managing programs and services. With the free and open source PMM built alongside Salesforce's NPSP, nonprofits can track any type of program or service, regardless of complexity or volume. **Nonprofit Cloud Case Management** Built on PMM, Nonprofit Cloud Case Management is a product that enables a nonprofit to track the programs and services delivered to clients who are engaging with the organization over the long term. It contains features such as: • Client Notes to track any updates based on interactions with clients • Case Plans which are a means to track the client's goals and action items that need to be completed to work towards those goals • Incident tracking, enabling organizations to capture any incidents the client has been involved with • Home Page for Case Managers to help them manage their day by highlighting tasks to be completed today, upcoming Events, any recent incidents, etc. • A customized view of the Contact Record to highlight the most important information that Case Managers need to know about their clients

Service Name	Service Description
Salesforce.org (continued)	**foundationConnect** foundationConnect is a grants management system for grant makers built on the Salesforce constituent relationship management platform. Grant makers can manage the entire lifecycle of philanthropic giving – from eligibility and application, to application reviews and evaluations, all the way through grants distribution and real-time outcome tracking. Through a portal, grantees can search for, save, and submit grant applications, collaborate and update status reports, and provide programmatic outcomes on an ongoing basis. **Grants Management** With Grants Management, grantmakers have a single system built off of the Salesforce CRM to simplify and accelerate grantmaking while facilitating greater collaboration between giver and recipient. Grants Management helps foundations and nonprofits who disburse awards and grants a simple way to track, manage and deliver funding programs. Grantees can easily find and apply for grants through an additional grantee portal, engage directly with grantmakers and share outcomes. Grantmakers can spend less time on tedious processes that bog them down and more time driving their philanthropic mission. **Education Data Architecture (EDA)** Developed in collaboration with partners and customers in Higher Education, EDA is an open source, community-driven data architecture and set of practices designed to configure Salesforce out of the box for higher education. As the foundation of Education Cloud, EDA provides a flexible and scalable framework to capture a 360-degree view of students from day one. **Student Success Hub** Built on EDA, Student Success Hub connects the people and systems to empower current and incoming student success conversations across campus by bringing student data – even legacy data – together to deliver a 360-degree view of the student across the entire institution.

Service Name	Service Description
Workplace Command Center	The Workplace Command Center provides a single source of truth for managing the complexities associated with maintaining workplace and employee safety and wellbeing. From the Workplace Command Center, organizations can send wellness surveys and assess wellness trends to uncover insights. Then, they can make informed decisions around workplace operations, while keeping employee health data secure. With the Workplace Command Center, organizations can quickly deliver custom learning to skill up employees for new ways of working, access prebuilt content kits on best practices, and gain data insights on employee learning. In addition, organizations can create new capacity models to reduce office density. Organizations can avoid large groups in common areas, office spaces, or elevators through spatial distancing and scheduling breaks. The Employee Wellness Check is a platform to help organizations prioritize safety and wellbeing. Employee Wellness helps enable leaders to make informed decisions on workplace operations by making critical employee, workplace, and public health data accessible. Securely monitor employee health and safety with wellness surveys.
Platform Events (including Change Data Capture)	Platform Events enables developers to deliver secure, scalable, and customizable event notifications within the Salesforce platform or from external sources. Customers use Platform Events to connect business processes in Salesforce and external apps through the exchange of real-time event data. Platform Events are based on a publish-subscribe architecture, and apps can publish platform events by using Apex or one of the Salesforce platform APIs (SOAP, REST, or Bulk API). In addition, declarative tools such as the Lightning Process Builder or Cloud Flow Designer can publish platform events. Change Data Capture is a streaming product on the Lightning Platform that enables customers to efficiently integrate Salesforce data with external systems. With Change Data Capture, customers can receive changes of Salesforce records in real-time and synchronize corresponding records in an external data store. Change Data Capture publishes events for changes in Salesforce records corresponding to create, update, delete, and undelete operations.

Service Name	Service Description
Salesforce Identity	Salesforce Identity delivers identity and access management (IAM) services directly from a Salesforce org. With Salesforce identity services, customers can authenticate users across orgs, Experience Cloud sites, and digital channels to provide authorized access to data. Additionally, Salesforce Identity is built on the Salesforce Platform and provides administrative tools for managing authentication as well as monitoring, maintaining, and reporting user apps and user authorization.
Service Cloud Voice (SCV)	Service Cloud Voice (SCV) is a Computer Telephony Integration solution natively integrated inside Service Cloud that offers streamlined customer service, Omni-Channel visibility for managers, and AI-driven insights for a phone-based service experience. SCV allows integration with cloud telephony and digital conversations within the agent workspace. SCV leverages real-time call transcription to unlock AI powered productivity tools. SCV makes it possible for supervisors to view calls and insights in real time to facilitate training and onboarding.
Salesforce Order Management (SOM)	Salesforce Order Management (SOM) is a customer-centric OMS built to deliver post-purchase journeys. With Salesforce Order Management, Customers can fulfill, manage, and service orders at scale by connecting B2C Commerce and their Core Services (e.g., Service Cloud) together for a 360-degree end customer experience.
Content Management System (CMS)	Salesforce Content Management System (CMS) is a simple, flexible and customer-first content management system. Built on the Salesforce Platform, Salesforce CMS empowers every team to create, manage and deliver relevant content at every touchpoint, from marketing, to commerce, service, and more.
Salesforce B2B2C Commerce	Built natively on the Salesforce platform, Salesforce B2B2C Commerce enables B2B companies to quickly launch a connected, direct-to-consumer (D2C) ecommerce storefront with clicks, not code. Now, companies that sell through distributors and retailers can capture that first-party data, enabling them to better understand their full customer base, connect directly with marketing, sales and service and in turn unlock a new revenue stream.
Net Zero Cloud (formerly branded as Sustainability Cloud)	Customers can gain critical insights about their carbon footprint with Net Zero Cloud. Using global emission factors to calculate greenhouse gas emissions, the app helps customers collect, categorize, analyze, and report energy usage data throughout their organization's business activities. Because it's built on top of the Salesforce Platform, you have access to tools that facilitate collaboration, project management, and reporting.

Service Name	Service Description
Loyalty Management	Loyalty Management, built on the Salesforce platform, helps organizations deliver innovative programs for customer recognition, reward, and retention. Loyalty Management is a unified, cross-industry solution that offers a host of features that enable you to plan and design loyalty programs, manage members, and partners. You can also track members' activities, reward members, drive engagement, and launch innovative promotions and offers.
Mobile Publisher	Mobile Publisher is a platform to transform Digital Experience sites, portals, and other Salesforce experiences into fully branded and customized mobile iOS and Android app experiences, all with no code and delivered directly to the Apple and Google Play App Stores.
Messaging for In-App and Web	Messaging for In-App and Web allows customers to elevate traditional chat interactions with rich, asynchronous experiences. Whether deploying chat in mobile apps with the In-app SDK, or on a website with the embedded experience, Salesforce customers can support their customers continuously. Messaging for In-App and Web supports modern conventional capabilities with AI-powered chatbots, rich content, read & delivery receipts, and attachments, directly in the conversation.
Subscription Management	Subscription Management is a business framework that uses tech-driven automation and shared data to optimize how to deliver subscriptions (where customers pay on a recurring basis for access to a product or service). It enhances customer experiences across the buying journey, driving adoption, renewals, retention, and growth.
Employee Productivity	Employee Productivity is a set of employee-facing features that, coupled with Employee Service agent capabilities, comprises the Employee Service solution. Employee Productivity empowers employees to seek help from HR, IT, legal, facilities and other employee-facing departments. Within the Employee Workspace, users can search for knowledge, log tickets, request service, engage chatbots, and communicate with agents.

Service Name	Service Description
Digital Process Automation (Including Decision Tables, Data Processing Engine, OmniStudio, Business Rules Engine, and Document Generation)	**Decision Tables** Define decisions or actions based on a collection of business rules that consider multiple inputs and outputs to decide the outcome for records in the Salesforce org or for the values that customers specify. **Data Processing Engine** Data Processing Engine helps customers transform data that's available in the Salesforce org and write back the transformation results as new or updated record(s). Customers can transform the data for standard and custom objects using Data Processing Engine definitions. **OmniStudio** OmniStudio provides a suite of services, components, and data model objects that combine to create Industry Cloud applications. Create guided interactions using data from your Salesforce org and external sources. With OmniStudio, customers may be enabled to create: • OmniScripts, which contain the user-interaction logic. • DataRaptors, which transfer and transform data between Salesforce and the OmniScripts, FlexCards, and Integration Procedures tools. • Integration Procedures, which bundle server-side data integration operations for efficiency and reuse. • FlexCards, which display data and launch actions. Note: This report addresses OmniStudio components built on Salesforce Services. The OmniStudio managed package that Digital Process Automation leverages is covered in the Vlocity SOC Reports. **Business Rules Engine (BRE)** BRE enables agile and automated decisions in digital processes for any industry. BRE provides Visual Rules Builder for customers to design or modify business rules. Industry Clouds may integrate BRE into their solutions to provide automated decisions that can be directly modified by the business users. **Document Generation** Intake, track, review and collect signatures for documents. Document Generation enables the merging of text-based formats (word/ppt) with data sources to create a range of customized documents, such as contracts, proposals, quotes, reports, etc. Merge fields from Salesforce objects when generating documents at runtime and share documents with your customers. Note: This report addresses Document Generation components built on Salesforce Services. The OmniStudio managed package and Vlocity managed packages that Digital Process Automation leverages are covered in the Vlocity SOC Reports.

In addition to the services as noted in the table above, this report also addresses Infrastructure Support and Management services (including related backups, encryption, change management, logical security, etc.) and Application Development and Change Management services (including change testing, approvals, implementation, etc.) that support various services provided by other Business Units as specified in the Salesforce Business Unit specific SOC examination reports.

Additional services not covered by the preceding description of the Covered Services above are out of scope of this report.

Overview of Salesforce Services' Covered Services Architecture

The Covered Services are operated in a multitenant architecture that is designed to segregate and restrict Customer Data access based on business needs. The architecture provides logical data separation for different customers via customer-specific unique identifiers and allows the use of customer and user role-based access privileges. Additional data segregation is maintained by providing separate environments for different functions, including for testing and production.

The System Engineering group manages the Instance (also referred to as Point of Delivery or POD), which refers to the Salesforce Services' Covered Services system layer deployed in secure high-availability data centers. Multiple customer environments are hosted in a single, self-contained POD that contains all the necessary servers, network equipment (e.g., IDS, firewall, VLAN switch), and disk storage hardware. Redundant system components and optimized design patterns maximize availability and performance.

Services Provided by Subservice Organizations Excluded From the Scope of the Examination

The Covered Services use the following Subservice Organizations in order to provide services to customers:

Subservice Organization	Description
Salesforce Corporate Services	Corporate level controls and services provided by Salesforce, Inc.
Amazon Web Services (AWS)	Infrastructure as a Service (IaaS) hosting Covered Services is provided by AWS. Data centers are in the following locations: • Montreal, Canada • Sydney, Australia, • Camden, Australia • Northern Virginia, USA (Salesforce Private Connect) • Oregon, USA (Salesforce Private Connect) • Frankfurt, Germany

Subservice Organization	Description
Heroku Services	Heroku provides Platform as a Service (PaaS) hosting for certain Covered Services. To determine which Covered Services utilize Heroku as a Sub-processor refer to the Infrastructure & Sub-processors (I&S) documentation linked within the Salesforce Services Security, Privacy, and Architecture (SPARC) documentation.

Locations and Infrastructure

Salesforce has the following key functions and locations which support the Covered Services:

Function	Description
Production Colocation Data Centers	Production data centers are in the following locations: • Ashburn, Virginia, USA • Sterling, Virginia, USA • Manassas, Virginia, USA • Chicago, Illinois, USA • Irving, Texas, USA • Frankfurt, Germany • Kobe, Japan • London, UK • Paris, France • Phoenix, Arizona, USA • Tokyo, Japan
Research and Development (R&D) Colocation Data Centers	R&D data centers are in the following locations: • Phoenix, Arizona, USA • Chicago, Illinois, USA
Operations Support	Operations support is in the following locations: • San Francisco, California (Headquarters), USA • Burlington, Massachusetts • Bellevue, Washington, USA • Northern Virginia, USA • Hyderabad, India • Dublin, Ireland • Singapore, Singapore • Sydney, Australia

Function	Description
Public Cloud Service Providers	Some Services have infrastructure hosted on the following public cloud service providers: • Amazon Web Services (AWS) • Heroku, Inc. (on Amazon Web Services, Inc.)

More information regarding the specific infrastructure, locations, and controls is contained within the Salesforce Services Trust and Compliance documentation on https://trust.salesforce.com/en/trust-and-compliance-documentation/. For further details on this section with regards to controls supported by Corporate Services and Heroku Services, please refer to the Salesforce Corporate Services and Heroku Services SOC reports.

Software

The following table details the key software and network components, which support the Covered Services.

Component	Description
Operating Systems	Operating Systems used to support the Covered Services are Linux.
Databases	In-scope Customer databases are Apache, Oracle, and Salesforce databases.
Monitoring Systems	There are multiple monitoring systems in use for the Covered Services, including: • Security incident event monitoring • Performance monitoring system
Network Infrastructure	The Covered Services network infrastructure utilizes a common set of network components, including: • Switches • Load Balancers • Firewalls • Routers • Hardware appliances

For further details on this section with regards to controls supported by Corporate Services and Heroku Services, please refer to the Salesforce Corporate Services and Heroku Services SOC reports.

People

The following teams are in-scope for this report as their job responsibilities require that they have access to production systems, develop code to be included into the environment or support operational and advisory functions:

Team	Responsibilities Covered
Security	Salesforce Services shares a number of security responsibilities with the Salesforce Corporate functions. Specific security team responsibilities can be found in the Salesforce Corporate Services SOC report.
Infrastructure Engineering	For Systems: • Server configuration & management • Setup access to servers For Network: • Network device configuration & management • Setup access to network • Define network security standards • Implement and review access control lists for network • Capacity planning • File attachment storage • Site switching/Disaster recovery
Database Engineering	• Database configuration & management • Setup access to database instances • Data protection
Development/Quality Engineering	• Develop new code, fix bugs • Release management • Write technical specifications and performance software build services
Program/Product Management	• Provide development project/product management, release/deployment management, and status reporting. • Identify customer requests and prioritize functionality to be released.
Site Reliability (SR) Engineering	• Provide Performance Incident Management for critical incidents within the Salesforce environment.

Team	Responsibilities Covered
Salesforce Corporate Services	• Salesforce Board of Directors • Hiring Practices and Staff Development • Security Awareness and Training • Risk Management • Monitoring of Internal Controls • Physical Security • Environmental Safeguards • Vendor Audit Program • Logical Security • Corporate IT Network Architecture and Management • Endpoint Protection • Product Security • Threat and Vulnerability Management • Security Monitoring • Incident Management • Contingency Planning and Business Continuity

For further details on this section with regards to controls supported by Corporate Services and Heroku Services, please refer to the Salesforce Corporate Services and Heroku Services SOC reports.

Procedures

Salesforce has detailed information security, availability, and confidentiality standards which are designed and categorized as per the National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4 control families, including:

- Access Control
- Audit and Accountability
- Awareness and Training
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection

- Personnel Security
- Physical and Environmental Protection
- Planning
- Program Management
- Risk Assessment
- Security Assessment and Authorization
- System and Communications Protection
- System and Information Integrity
- System and Services Acquisition

Customer Data

Customer Data is defined within the publicly available MSA. Customer Data processed on behalf of customers has been classified as Mission Critical, which is the highest sensitivity classification at Salesforce. Customer Data, as referenced in this report, is processed in accordance with Salesforce's role as a Processor as defined in the Data Processing Addendum (DPA) to the MSA.

The use cases for Customer Data extraction by Salesforce personnel are aligned with the customer MSA. Per MSA and documented processes, Customer Data extraction requests for technical support are reviewed and approved prior to execution, and extractions are documented, tracked, encrypted, and restricted for use by authorized personnel.

System Incident Disclosures

There were no incidents noted during the examination period that caused the Covered Services to not meet their security, availability, and confidentiality commitments.

Relevant Changes

The following table details the relevant changes to the Covered Services during the examination period:

Change	Description of Change
Covered Services	Inclusion of Digital Process Automation (Including Decision Tables, Data Processing Engine, OmniStudio, and Document Generation), Employee Productivity (formerly IT Service Center – Agent and Employee Service – Agent), Messaging for In-App and Web, and Subscription Management in scope of Salesforce Services' Covered Services System. Removal of Orchestrator as a named service in the Salesforce Services' Covered Services SOC reports as it is a feature of the in-scope Lightning Platform. Removal of Einstein Prediction Builder, Einstein Case Classification (formerly branded as Einstein), Einstein Language, and Einstein Vision as named services in the Salesforce Services' Covered Services SOC reports as these services are included within the scope of the Einstein Platform, Einstein Platform on Hyperforce and Einstein AI SOC reports.
Onboarded Identity Lifecycle Management (ILM) Tool	As of July 1, 2022, production assets including servers, databases, and network devices rely on the ILM for provisioning and deprovisioning of user access, facilitation of user access reviews, and monitoring of access record data in the ILM tool if it diverges from the actual state of access in a target production asset.

Relevant Aspects of the Control Environment, Risk Management, Monitoring, and Information and Communication

As defined by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), internal control is a process affected by an entity's board of directors, management, and other personnel. Internal control consists of five interrelated components:

Component	Description
Control Environment	This sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline, and structure.
Risk Management	This is the entity's identification and analysis of risks relevant to the achievement of its objectives, forming a basis for determining how the risks should be managed.
Monitoring	The entire internal control process must be monitored, and modifications are made as necessary. To support modifications, the systems react dynamically and change as conditions warrant.

Component	Description
Information and Communication	Surrounding these activities are information and communication systems. These enable the entity's people to capture and exchange information needed to conduct and control the entity's operations.
Control Activities	Control policies and procedures must be established and executed to help ensure that the actions identified by management are completed as necessary to address risks for achievement of the entity's control objectives.

Set out below is a description of the components of internal control related to the Covered Services that may be relevant to customers.

Control Environment

The control environment begins at the highest level of the Company. Executive and senior management play important roles in the Company's tone from the top, and their direct leadership is an integral part of the integrity and ethics, which are part of the corporate culture. For further details regarding this section, please refer to the Salesforce Corporate Services SOC report.

Salesforce Board of Directors

The Salesforce Board of Directors (BOD) maintains corporate governance guidelines that outline the roles, responsibilities, limitations, and operation of the BOD. For further details regarding this section, please refer to the Salesforce Corporate Services SOC report.

Hiring Practices and Staff Development

The Salesforce Employee Success team, and Security Communications and Engagement team for security related training, are responsible for hiring practices and staff development. These activities include:

- Background investigations
- Employment offer acceptance
- Employment disciplinary action
- Security awareness and training
- Employee performance reviews

For further details regarding this section, please refer to the Salesforce Corporate Services SOC report.

Risk Management

Salesforce's Enterprise Strategy, Enterprise Risk Assessment, and Security Risk Assessment processes are detailed in the Salesforce Corporate Services SOC report.

Monitoring

Salesforce's Security GRC team is responsible for monitoring of internal controls and coordinating third-party assessments over the controls for the Covered Services. For further details regarding this section, please refer to the Salesforce Corporate Services SOC report.

Information and Communication

Salesforce maintains an Enterprise-wide internal Information Security Policy, supported by detailed security standards and training to ensure that employees understand their individual roles and responsibilities regarding security, availability, confidentiality, and significant events.

For further details regarding this section, please refer to the Salesforce Corporate Services SOC report.

Control Activities

General Information Systems Controls

Salesforce maintains a formal Company-wide information security management system (ISMS) that conforms to the requirements of the ISO 27001 standard and NIST Cybersecurity Framework (CSF), including security policies, standards, and procedures. Formal policies and procedures are documented for operational areas including: data center operations, development, program management, production management, infrastructure engineering, quality engineering, release management, operations, hiring, and terminations. The Information Security Policy has been developed to define the information security objectives of the Company, which are supported by security standards.

Physical Security

The Salesforce Physical Security team is responsible for physical security measures at the Corporate Offices, and components of physical security at colocation data center facilities. Further details of physical security at Salesforce Corporate Offices and colocation data center facilities are found in the Salesforce Corporate Services SOC report.

Physical security at public cloud service providers is the responsibility of the public cloud service provider. Refer to “Complementary Subservice Organization Controls” for more information.

Vendor Audit Program

The Salesforce Security GRC team includes a Vendor Audit Program (VAP) for evaluating and monitoring technical support vendors, data center hosting providers, sub-processors, and public cloud service providers. For further details regarding this section, please refer to the Salesforce Corporate Services SOC report.

Logical Security

The Information Security Policy and its supporting security standards, which have been reviewed and approved by management, specify the minimum standards for logical access to Salesforce systems. The standards also identify functional responsibilities for the administration of logical access and security, and the classification of data.

Account Provisioning

Approval for a new employee’s standard user account must originate from the Hiring Manager and is based on the employee’s job function. Subsequent accounts used to access the Salesforce Services’ Covered Services system is restricted to authorized personnel. Access is provisioned according to the principle of least privilege, and separation of duties is enforced.

A subset of production access to servers, databases, and network devices can only be requested via a self-service Identity Lifecycle Management tool (ILM) once users have satisfied a set of predefined requirements. These requirements include a completed background investigation, completion of change management training, completion of Government Cloud training (for access to the Government Cloud environment), acknowledgement of cryptographic key custodian responsibilities, and provisioning of a multi-factor authentication (MFA) device. Once the prerequisites are met, an access request can be submitted for the user requiring access. Upon submission of an access request, the ILM tool routes the case to authorized approvers as configured in the tool. Once approved, the tool automatically provisions the access to target systems, except for the Government Cloud environment wherein production access is manually provisioned.

The ILM tool was initially designed to allow users with Administrator privileges to self-approve ILM cases. The system was designed this way to support with:

- Migration of authorized user access data from existing systems to ILM which required approved ILM cases
- Providing user support in the event of issues with approvers or routing
- Pre-go live / pilot testing for new system to be onboarded to ILM
- End-to-end regression testing after major release of the ILM tool and any supporting tools.

As of September 21, 2022, the company has modified the system to remove the ability for Administrators to self-approve ILM cases.

To validate the efficacy of the automated access provisioning functionality within the ILM tool, management performs an access provisioning look back at least semi-annually to ensure that the access requested and approved was provisioned correctly. Additionally, as a part of this process, management reviews access requests on a sample basis to ensure that the automated workflows correctly routed access requests to the appropriate and authorized approvers. Any discrepancies identified are investigated and remediated.

For assets that are not utilizing the ILM tool, user access to the covered services system are manually provisioned.

Production servers are configured to log escalation of privileges. In addition, network devices and servers log successful and unsuccessful account logon events and transmit them to a log aggregation facility where logs are retained for a period of one year. Logical access controls restrict access to the Covered Services' production system logs and protect audit information from unauthorized modification and deletion.

Vendor-provided database accounts that are not needed or used are locked or removed. For database accounts that remain, the default passwords are changed. Only database administrators have access to privileged database accounts. Database human user accounts are automatically locked once passwords are expired.

Internal Admin Portals are used to maintain application service health and to provide support for customers. The License Management Internal Admin Portal is used by the following Covered Services: Salesforce Configure Price Quote (CPQ), Salesforce Billing, B2B Commerce, Industry Clouds, Workplace Command Center, Employee Productivity, and Salesforce.org. All other Covered Services use the Standard Internal Admin Portal.

Access to Internal Admin Portals require approval prior to access being granted, with the following exception: Salesforce Configure Price Quote (CPQ), Salesforce Billing, and B2B Commerce Internal Admin Portals access is granted by default based on the user's role within the organization.

Public cloud environments are created with a set of predefined Salesforce Security approved Identity Access Management (IAM) roles, which are configured via the public cloud provider's API. At the time of environment provisioning, these predefined configurations are automatically applied to ensure account owners adhere to security standards and permission boundaries. Custom IAM roles may be created by account owners and assumed by users for console access but the roles are required to conform to existing service control policies, unless Security Assurance approval has been granted. Access to the public cloud management console is managed via a just-in-time (JIT) dashboard and requires approval from an authorized administrator for the environment and resources for which access is being requested. Users can only request access to a predefined IAM role approved by Salesforce Security. Each request is only valid for a defined period of time in which the user can access the console, and the access can also be immediately revoked if needed.

Customer access is the responsibility of the customer. New customers sign/acknowledge a MSA, which includes security considerations for protecting the security, confidentiality, and integrity of data. A designated Salesforce system administrator provides customers access to their environment and subsequent users are provided access by the customer's system administrator.

The MSA also specifies the responsibilities of the users and Salesforce's responsibilities and commitments.

Upon acceptance of the MSA, the customer is responsible for the administration and maintenance of access to the system for their personnel, as well as ensuring the security settings, such as password settings, are configured in accordance with their specific policies and procedures. Further details of MSA requirements are found in the Salesforce Corporate Services SOC report.

For details on Salesforce Heroku Services platform account provisioning, please refer to the Heroku Services SOC report.

Access Authentication

Access to the production infrastructure is restricted to authorized personnel based on assigned roles. Privileged system access is restricted to a limited number of system administrators and their management. The password-based authentication, use of MFA, and dynamic password generation or password parameters used to access production systems are set in accordance with company standards.

Users can access production systems by first authenticating to the corporate network, via a secure private connection solution, and then authenticate through multiple access control points described below as applicable:

- The first layer of authentication is through a secure virtual gateway and requires multi-factor authentication using their username and a one-time passcode token.
- The second layer of authentication includes authentication to the bastion host using their username and a one-time passcode token.
- The third layer is authentication to the individual production systems where the user must log in with their username and password on the target system.

Access to the public cloud management console is role-based, and is managed via a just-in-time (JIT) dashboard and requires approval from an authorized administrator for the environment and resources for which access is being requested. The access is restricted to a defined period of time in which the user can access the production environment, and is automatically revoked when it reaches expiry. Additionally, users access the Public Cloud Infrastructure and Private Connect production environment after authentication to the corporate network, via a secure private connection solution, and must pass through multiple layers of authentication as described below:

- The first layer of authentication is through a secure virtual gateway and requires multi-factor authentication using their username and a one-time passcode token.
- The second layer is authentication to the public cloud console JIT dashboard where the user must log in with their username and password as well as a one-time password token.
- The Third layer of authentication includes authentication to the public cloud management console which requires a JIT access request and approval through the public cloud console JIT dashboard. Once approval is granted, the user is provided with temporary credentials for authentication to the public cloud management console.

Authentication credentials are obscured during the authentication process. Internal system management functionality is segregated within the production environment using various layers of security within network devices, the operating system, databases, and the application.

Users are authenticated to the Salesforce Configure Price Quote (CPQ), Salesforce Billing, B2B Commerce, Industry Clouds, Workplace Command Center, Employee Productivity and Salesforce.org License Management Internal Admin Portals through federation with Active Directory.

Policies and agreements are in place that define the circumstances in which customer data can be used, including requirements to limit removal of the data from its native storage and requirements for maintaining the security of the data at all times. Sessions into the secure virtual gateway and Secure Shell (SSH), which are used to access production, are automatically terminated after a determined number of inactive minutes to prevent unauthorized activity or use.

For details regarding the access authentication in Salesforce Heroku Services platform, please refer to the Heroku Services SOC report.

Access Reviews

Logical access to production environments is reviewed on a quarterly basis to verify the appropriateness of users within the systems that support the Covered Services. In addition, management performs an access review of the users with the ability to grant users JIT access into the public cloud administration console to ensure access rights remain appropriate based on job functions. For each quarterly review, a ticket is created to track and to monitor the completion of each review process.

The ILM tool assists in the facilitation of user access reviews. Each user role, or entitlement, has a predefined role owner assigned in the ILM tool. Role owners, or direct managers, depending on if the access review is configured for role owner or manager review, will receive a notification a list of users they are responsible for reviewing. Any users that are identified as not appropriate will be rejected by the reviewer, and user access is automatically removed by the ILM tool.

For assets that are not utilizing the ILM tool, logical access is reviewed on a quarterly basis by teams owning the systems that support the Covered Services to verify that terminated users have been removed from the respective systems through an internal ticketing system and access remains appropriate based on their job function. For any discrepancies found during the access review, the responsible employees must correct and document the removal. Once the results of the access review are documented, there is a second-line review by an application, service or system owner or direct manager or director; once the second-line approves the findings, and confirms remediation of the findings, the quarterly access review ticket is then closed.

A subset of production assets (i.e. applications, servers, databases, and network devices) rely on the ILM tool to initiate an ad-hoc user access review when an individual changes job functions. The Identity Lifecycle Management tool is configured to raise the transfer review case and assign it to the receiving manager of the transferred individual. Any rejected access by a user's new manager is removed. Furthermore, if there is any access that is neither approved nor rejected by the transferring user's manager, the access is automatically removed after a period of time defined in the system, in accordance with Salesforce Security Standards.

For details regarding the access review in Salesforce Heroku Services platform, please refer to the Heroku Services SOC report.

Access Removal

In the event that a Salesforce employee or contractor leaves the organization, the individual's Manager or Employee Success representative (on behalf of the manager) is responsible for initiating the termination in the Human Resources Information Systems (HRIS). When a worker's termination date is reached, the identity lifecycle management tool initiates automated access removal processes to remove the terminated user from the relevant target assets in accordance with timeliness requirements in Salesforce Security Standards.

For assets that are not utilizing the ILM tool, user access to the covered services system are manually removed in a timely manner. Corporate network access is removed within two business days of termination task creation. Production access that has downstream authentication mechanisms, in addition to corporate network access, is removed within five business days of termination task creation. Production network access that is not gated by the corporate network is removed within two days of termination task creation.

For production access that does not have downstream authentication mechanisms, access is controlled through Active Directory Single Sign On (SSO) and relies on corporate network access removal.

Prior to the ILM access deprovisioning process onboarded on July 1, 2022, in parallel with the automated termination task created, a job was executed which systematically removes a user's infrastructure access where technically feasible. In the event of a failure in the automated job, an alert was sent to the Lifecycle Identity Management Engine team (LIME). The issue was then investigated and if determined to be a true issue, a ticket was created to document actions to resolve the issue.

For the Government Cloud environment, access is removed within one business day of automated termination task creation.

For production access that does not have downstream authentication mechanisms, access is controlled through Active Directory Single Sign On (SSO) and relies on corporate network access removal.

For further details regarding this section, please refer to the Salesforce Corporate Services and Heroku Services SOC reports.

Data Divergence and Data Quality

The Salesforce ILM tool is configured to monitor the current state of access on a subset of production assets and trigger alerts when access record data in identity lifecycle management tool diverges from the actual state of access in a target production asset. Access data divergences, if any, are investigated and remediated on a timely basis.

To address risk of inappropriate access to production assets due to data quality differences between the HRIS and the ILM tool, an analysis is performed on a quarterly basis to detect termination and transfer events that are not successfully triggered in the Salesforce ILM. If any events are identified, further investigation is performed and the identified events are resolved in accordance to the agreed upon service level agreement after the end of a quarter. For the subset of production assets utilizing the ILM tool, corporate network access is required as an initial primary layer of authentication. This additional layer of defense protects against unauthorized user access to production after termination. Further details about the corporate network access termination process can be found in the Corporate Services SOC report.

Password Requirements

The password requirements for corporate and production systems are required to meet or exceed the following information security password requirements defined in Salesforce's Authentication Standard, which includes:

- Passwords must have a minimum length of:
  - 12 characters for production systems
  - 16 characters for corporate endpoint systems and applications
  - 20 characters for service accounts
- Password complexity must contain three of the following four characters: uppercase, lowercase, numbers, and symbols based on available system functionality.
- Password maximum lifetime is restricted to 365 days for corporate endpoint systems and applications.
- Password maximum lifetime is restricted to 90 days for administrators and production systems.
- Passwords cannot be reused for at least 6 generations.
- Account lockout settings are enforced after a number of consecutive invalid login attempts and automatically lock the account after the number of unsuccessful attempts is exceeded.

For further details regarding this section, please refer to the Salesforce Corporate Services SOC report.

Network Architecture and Management

The information system consists of three logically and physically separate networks: a corporate network, a R&D network, and a production network. The corporate network supports internal corporate functions and is separate from the production network, which supports customer instances.

For further details on Salesforce's Corporate and Heroku Services network, please refer to the Salesforce Corporate Services and Heroku Services SOC reports.

The R&D network supports software development, quality assurance, and part of release engineering. Access Control Lists (ACLs), firewalls, and subnets are used to prohibit network access and information flow between the different networks.

The data centers have a fully redundant infrastructure. Network devices are also implemented in a fully redundant, fault-tolerant configuration. Servers that require redundancy are configured with two separate switches, which are connected to separate network interface cards on each server.

Networking protocols that are not necessary for business purposes and/or are deemed to be non-secure are disabled. Protocols and allowed services are documented in configuration standards.

Tools are installed and used to monitor the status and load of each managed network device. The monitoring tools are configured to generate alerts when specified thresholds are reached or exceeded. When triggered, the predefined group of alerts will generate an automatic notification to designated personnel and, depending on the severity of the problem, appropriate levels of escalation are applied.

Boundary Protection

Mechanisms are employed within the network to monitor and control communications at the external boundary of the system. Border routers configured with access control lists are used to filter unwanted network traffic and can apply rate limits if necessary.

To protect the security of the network, proxies are configured to disable access to public emails, instant messaging, and other non-business functions from the production servers.

External network devices, configured to "deny all – allow by exception" are used to filter traffic and remediate basic Denial of Service (DoS) attacks. Salesforce production data center network traffic is also routed through a Distributed DoS (DDoS) protection service provider to limit the effect of DoS attacks.

Load balancers are used in conjunction with the internal network devices to encrypt/decrypt traffic, Network Address Translation is used for customer IPs, and customer traffic is routed to Virtual IPs rather than IPs within the network. The customer's real IP is inserted into the header so that the application recognizes the origin of the traffic.

Internal firewalls, routers, and switches are used to control traffic between Customer Instances (a multi-tenant stack). ACLs established on the network devices within the specific instances prevents user traffic from crossing instances. ACLs are configured to deny all and allow only explicitly defined connections and prevent the database hosts from accepting any traffic other than the expected database traffic. Application servers are configured to communicate only with specific instances of other resources, preventing unauthorized connections to other instances or back to the host. ACLs on the application servers are used to "whitelist" internal IP addresses for administrative functions within resources.

Network Access Controls

Network access controls and protocols are defined within the Salesforce's Network Protection Standard. Access to change network access control configurations is restricted to authorized personnel who have the required access and approval before making changes, which follows the change management process as described below.

Application Protection

Customers connect to the Covered Services over the Internet through their Salesforce instance and data transported into and out of these controlled environments is encrypted in transit. Once inside these controlled environments, customers can utilize the application framework and managed computing assets to store and manipulate data in their organizational instance.

Internal Admin Portals are used to maintain application service health and to provide support for customers. Authorized users provide operational support for products and features. Support personnel use the applications through special accounts to support customers and only have access to Customer Data when authorized by the customer. Customers granting access for troubleshooting purposes can define the duration of the access, activity is logged, and logs are available for customers' review. Setup audit trail tracks the date of change, who made it, and what change was made. For more details on Setup Audit Trail, please visit: https://help.salesforce.com/s/articleView?id=sf.admin_monitorsetup.htm&type=5.

With a multi-tenancy platform, the platform prevents unauthorized and unintended information transfer via shared system resources through logical access controls. Controls are in place to restrict user access across shared resources and equal security protections are provided to Customer Data. Hosted customers (organizations) are assigned an "Org" with an associated unique "OrgID" within the Salesforce infrastructure. Only the information associated with the OrgID assigned to the customer's credentials are available to the authenticated user.

Intrusion Detection

An Intrusion Detection System (IDS) monitors for potential security breaches. IDS devices are placed between the edge routers and aggregation layer (in front of the load balancers) and behind the load balancers to monitor network traffic, including malware events in Salesforce production data centers.

IDS events are collected and configured to generate IDS alerts to the corporate Security Detection and Response team as security events occur in the environment. Privileged access to administer the IDS is restricted to authorized personnel. For further details of Salesforce's security event log ingestion, centralized logging, alerting, and security event remediation, please refer to the Salesforce Corporate Services SOC report.

Note that the IDS is only currently applicable to the production and Government Cloud environments at Salesforce co-located data centers. Due to system limitations with the public cloud service provider, an IDS is not currently in place. In lieu of an IDS, Salesforce has implemented logging and netflow log collection (drops and accepts) for all ingress/egress traffic. The public cloud logs are analyzed and reviewed.

Malware and virus detection are in place at the corporate layer and alerts are generated in the event of compromise or potential compromise.

For further details on Salesforce's Intrusion Detection processes, please refer to the Salesforce Corporate Services SOC report.

Endpoint Protection

The Salesforce Business Technology team is responsible for managing anti-malware solutions, device encryption, and mobile device management software.

For further details regarding this section, please refer to the Salesforce Corporate Services SOC report.

Product Security

The Salesforce's Security team includes a function for Product Security. The Product Security function includes conducting Application Security Assessments, which are black-box web application penetration tests performed by independent third parties. In addition, Salesforce has an invite-only bug bounty program.

For further details regarding this section, please refer to the Salesforce Corporate Services SOC report.

Threat and Vulnerability Management

Vulnerability Scanning

Vulnerability scans are performed on both internal and external facing production systems (including hosts and network devices) using internal scanning resources on a periodic basis.

For further details regarding this section, please refer to the Salesforce Corporate Services SOC report.

PCI-DSS Penetration Testing

Bugs identified from penetration tests are assigned severity/priority rating, tracked and monitored through to remediation per the defined Service Level Agreements for vulnerabilities, in coordination with product engineering teams.

Vulnerability Tracking and Patching

New host and container base images are released at least monthly with the most recent operating system vulnerability patches and are available for service teams to apply to their infrastructure assets.

The Threat and Vulnerability Management team, in coordination with product engineering teams, utilize scanning and monitoring tools to identify and track vulnerabilities in hosts, containers, and third-party / open source code. Results are evaluated and included in the analysis performed as part of the overall risk assessment process.

For further details regarding this section, please refer to the Salesforce Corporate Services SOC report.

Encryption

Transport Layer Security (TLS) encryption is used to protect the confidentiality and integrity of information transmitted between the customer's web browser and the Covered Services.

Cryptographic keys for TLS certificates are monitored by the Security team for expiration. Follow-up procedures are performed with the Certificate Authority to renew Salesforce cryptographic keys expiring within 90 days.

The Covered Services offer multiple features for encryption of Customer Data at rest. With the Platform Encryption offering, customers can choose to encrypt sensitive data stored in custom fields, supported standard fields, Chatter, files, attachments, and emails. This is an additional paid feature. Salesforce also offers a free encryption feature, Classic Encryption, available for custom fields only that customers create. For more details on Platform Encryption and Classic Encryption, please visit: https://help.salesforce.com/articleView?id=security_pe_vs_classic_encryption.htm&type=5.

Classic and Platform Cryptographic Encryption keys are rotated with each major Salesforce release and secured during transmission and storage in accordance with the Cryptographic Key Management Standard. Customers are responsible for rotating their master keys or tenant secret keys depending on the selection of encryption offering.

For details regarding encryption of data in the Salesforce Heroku Services platform, please refer to the Heroku Services SOC report.

Change Management

The change management process supports a controlled framework as well as proper segregation of duties for the approval and implementation of changes. Salesforce's Change Management Standard outlines the activities to be performed during each phase of the change process, as applicable, and the supporting tasks that need to be completed for each activity.

Changes are implemented during scheduled maintenance windows for high-risk changes and planned maintenance to minimize customer impact unless required to address an urgent service issue. Low-risk, routine changes are reviewed by the Change Advisory Board (CAB) to be permitted to run as pre-approved once it is safe to do so. Requests for changes, as well as system and hardware maintenance, are standardized, categorized, and prioritized according to documented policies and procedures.

The change management processes above also cover the report building tools available to customers for analyzing data stored by the customer in the Covered Service.

Asset inventories of all production systems that reflect the current information system environment are documented and inventories are maintained at a level of granularity deemed necessary for tracking and reporting purposes. An asset inventory review of the Covered Services' production systems is performed periodically.

Current and prior configurations for production servers, network devices, and databases are maintained in order to support rollback based on the nature of change.

Infrastructure Change Management

The change management process requires the support of people, process, and technology. Individuals submitting infrastructure changes into production are required to follow the defined Global Change Management Process and Change Management Security Standard and to complete mandatory change management training before participating in the change management process.

The Global Change Management Process defines the required approvals that a change must route through before the change implementer can begin the change in production. Salesforce uses a ticketing system as the technology to support the change management process as defined in the Global Change Management Process.

The change management process identifies the roles and responsibilities of each of the members on the change process as well as the change types. Changes for infrastructure components are tested in a dedicated environment using production class equipment before being deployed into production, and a post-change verification is conducted. If testing cannot be conducted in a non-production environment, the change is applied to a minimal number of production devices and functionality is verified after implementation. Based on the nature of changes, additional steps are documented in the ticketing systems before changes are implemented into production: an assessment of risk and potential impacts, and rollback plans including procedures for recovering from unsuccessful changes of unforeseen events. Only authorized personnel can implement a change into the production environment.

Routine and periodic hardware maintenance is performed to reduce the frequency and impact of performance failures. Salesforce notifies customers of planned downtime through the Trust Maintenance page.

Infrastructure change management encompasses operational changes for maintaining the service at the hardware, server, network, and database level. The majority of changes that are processed via the Salesforce infrastructure change process are Standard or Standard Pre Approved changes that include routine system patching, firewall, and network changes necessary to maintain the underlying infrastructure supporting the services. These changes are considered lower risk, routine operating activities and either follow an established pre-approved template, require a peer review approval, or are systematically implemented based on a pre-approved change category prior to implementation.

There are five change types: Standard Pre-Approved, Standard, Minor, Significant, and Emergency Break Fix. Standard Pre-Approved changes are structured for repeatable execution. Standard Pre-Approved changes may be automatically implemented when the ticket is created as it follows a standard change template or change category and has been pre-approved via CAB. These are limited to low-risk changes and typically include patching or other operational activities that have a consistent history of success and execution without errors. Standard changes are low risk, performed frequently, and use a well-defined run list. Minor changes are deemed low to moderate risk. Significant changes are higher risk changes. Minor and Significant change types require Peer Approval and review from specific individuals in the related functional approval group and/or Change Management team and can be subject to a CAB review before approval. Emergency Break Fix changes are unplanned changes often in response to an event and require peer review and Executive approval. Database changes are a subset of infrastructure changes. This type of change includes changes to the database configuration and data maintained within the tables.

Application Change Management

Application change requests are documented and tracked through the online ticket management system and/or code repository. Desired application functionality and features are identified, prioritized, and initiated by product owners for future development. Information security and availability considerations are core components in application development and testing. Adaptive Development Methodology (ADM) and Scrum project management frameworks are used to manage application development and testing.

Application code changes undergo testing and/or peer review prior to merging the changes into the master code that makes up a release.

There are 3 types of releases: Major releases that include new product features, Patch releases that include fixes and upgrades following major releases, and Emergency releases to address issues and bugs.

There are 12 release groups for the Covered Services system: Salesforce Mobile (covers Salesforce Mobile App), Industries (covers Industry Clouds), QTC (covers Salesforce Quote to Cash), Workplace Command Center, Chat (component of service cloud), CRM Analytics (formerly branded as Tableau CRM), Salesforce Private Connect, B2B Commerce, Salesforce.org, Salesforce Order Management (SOM), Mobile Publisher, Employee Productivity, and Salesforce Core (other in-scope services).

For the release groups identified above, application releases into production do not occur until applicable sign-off is obtained from an Engineering Manager.

The sign-off from the required individuals must be documented in the associated release ticket, and is an indicator of successful testing of the changes and an approval to deploy the release.

Hybrid engineering is employed by Salesforce during the software development life cycle. Software engineers are cross trained to perform development and quality assurance roles. Segregation of duties is achieved by ensuring that application code development and quality assurance testing is performed by different individuals.

The change management tools (code versioning software and online ticketing system) maintain a record of changes, including the implementer's name, approvers' names, implemented solution, roll-back plans, and any issues arising from the change. Post change validation plans are created for each change to specify the steps that should be performed to validate a change after implementation in the production environment. The steps in the validation plan are executed by the change implementer to confirm the change was successfully executed in production.

Weekly release management meetings are held to discuss the current release schedule and milestones. Release notes are documented and communicated to internal and external users via the Trust site for changes and maintenance that affect functionality, features, system security, and availability. Details about maintenance windows include the maintenance time period, instance(s) impacted, and the reason for the use of the maintenance window.

For details regarding the changes to the system in the Salesforce Heroku Services platform, please refer to the Heroku Services SOC report.

Service Monitoring

The Covered Services and supporting infrastructure are monitored for availability and performance. A real-time alerting system will be triggered and alert on-call Engineering team members if defined reliability, availability or performance thresholds are exceeded.

Various automated and manual systems are used to monitor the confidentiality, integrity, availability, and performance of the service, such as intrusion detection systems, performance and health systems, and security event correlation systems.

Security Monitoring

The Covered Services are also monitored for security purposes. The Salesforce Security Detection and Response team provides centralized monitoring for malicious activity, open vulnerabilities, and indicators of compromise. Servers, production network systems, public cloud control plane systems, and databases are configured to forward log data to a centralized Detection and Response system, which then uses predetermined thresholds and triggers to generate alerts.

Examples of security events that will trigger an alert include (but are not limited to) unauthorized attempts to access production infrastructure, unpatched infrastructure, and application vulnerabilities. Additionally, servers are configured to log privileged operations (sudo) undertaken on the platform in order to provide an audit trail and increase accountability. For further details regarding this section, please refer to the Salesforce Corporate Services SOC report.

Incident Management

Salesforce Services performs incident management in three major categories:

- Security Incident Management
- Availability Incident Management
- Customer Incident Management

Security Incident Management

Security incident management is performed by the Salesforce Computer Security Incident Response Team (CSIRT).

For further details regarding this section, please refer to the Salesforce Corporate Services SOC report.

Availability Incident Management

Personnel in offices worldwide support the continuous operations of Salesforce. The environment is monitored 24/7 through a follow-the-sun customer support model for reliability and performance. The Site Reliability team provides site monitoring, first response, and proactive triage and resolution. The SR team handles first and second tier support, with infrastructure engineers providing escalation support. Monitoring tools are automated and route potential issues, and problems to the SR team.

All production and sandbox instances are monitored in real time. Customer impacting performance incidents are documented in an online ticketing system. Each incident is assigned a severity level to prioritize importance and the direct resources assigned to those issues of greatest impact to the system.

Formal incident handling capabilities for system performance incidents are implemented, which include preparation, detection, analysis, containment, eradication, and recovery. Investigation and corrective actions for performance incidents are documented and shared with key personnel to confirm corrective actions have been completed and lessons learned have been incorporated.

Internal and external users can access the Salesforce Trust site at any time, which contains information around service disruptions, system availability, informational messages, and daily metrics around performance issues.

High-level performance and availability reports are produced and discussed during monthly executive management meetings.

System capacity for long term strategic planning is monitored on an ongoing basis. Capacity planning tools are used to assess performance (such as usage and growth) across Salesforce instances and plan for remediation based on the risk analysis and forecasting.

For details regarding the availability of incident management in the Salesforce Heroku Services platform, please refer to the Heroku Services SOC report.

Customer Incident Management

The Covered Services utilize the Salesforce Enterprise Customer Support processes.

For further details on Customer Incident Management and Support, please refer to the Salesforce Corporate Services SOC report.

Backup, Recovery, and System Availability

A combination of near real-time data replication and data backups are utilized to protect Customer Data. Data centers are configured in pairs, so primary production infrastructure and production data are fully replicated to secondary sites.

The mirror site is a passive site containing equal (or more) capacity of the production data center, as the systems are the same as the primary. Customer Data in application databases is backed up using incremental backups, which are merged daily to create full backups, and hourly archive log backups. Database backups of customers' production data are retained for a minimum of 90 days and backups of customers' test data (sandboxes) are retained for a minimum of 30 days. Attachments which reside on Fileforce servers are replicated and/or backed up. On customer attrition, attachments on Fileforce servers are purged after 90 days in production and sandbox instances. Customers should take action to retain data they deem important.

Formal processes and procedures to securely dispose of any device that may contain Customer Data including backup media and hard drives have been developed. The media management procedures apply to all data center environments and include procedures for physical destruction.

Backup media does not leave secure data center facilities until the media is securely wiped and destroyed through a secure destruction process.

A Disaster Recovery Plan outlines the actions to be followed to meet availability and system requirements. The Disaster Recovery Plan includes, among others, details regarding recovery time objectives, key personnel, and recovery processes to be followed in the event of a declared disaster. Salesforce will test its disaster recovery plan at minimum on an annual basis and will continue to enhance and develop processes and its technology related to disaster recovery to further reduce Recovery Point Objective (RPO)s and Recovery Time Objective (RTO)s.

In addition, Salesforce Private Connect, which creates a native, secure integration between AWS and Salesforce, is configured and deployed in a highly available manner in AWS to meet availability and system requirements in the event of a business impact disaster. Private Connect is configured to be spread across multiple availability zones and regions, where possible.

Further, disaster communication processes are exercised using the mass notification system during each exercise, which includes call-outs with response requests to Salesforce's Global Crisis Management Team (CMT) and the Site Reliability Teams. Service agreements are in place for each of the alternate processing facilities and failover to the alternate processing facilities is logically controlled and does not require physical access to the production infrastructure to execute the failover.

In addition, each production data center is served by multiple Internet Service Provider Internet connections using a carrier-class model in order to provide redundancy. Further details on Internet Service Provider redundancy in data centers can be found in the Salesforce Corporate Services SOC report.

For details regarding the backup, recovery and system availability in Salesforce Heroku Services platform, please refer to the Heroku Services SOC report.

Contingency Planning and Business Continuity

In addition to the Salesforce Services Disaster Recovery Plan, Salesforce has the following enterprise-wide functions:

- Global Business Continuity Program (BCP)
- Business Impact Analysis (BIA)
- Global Crisis Management Team (CMT)

For further details regarding this section, please refer to the Salesforce Corporate Services SOC report.

Customer Data Deletion

After termination of all subscriptions associated with an environment, Customer Data submitted to the Covered Services is retained in inactive status within the Covered Services for 120 days, after which it is securely overwritten or deleted from production within 90 days, and from backups within 180 days. There are two separate Customer Data deletion processes within the scope of this report executed in accordance with the timelines above and Salesforce Security, Privacy, and Architecture Documentation. The Core data deletion process, which deletes or overwrites Customer Orgs from organization databases, and a separate, manual process to delete in-scope Customer Data stored in Mobile Publisher.

On June 22, 2022 Salesforce implemented enhancements to the code that identifies Mobile Publisher attrited customer licenses for deletion to better align with SPARC commitments. Additional improvements were made to the data deletion process which includes steps to identify in-scope orgs ready for deletion and validate deletion executed successfully in accordance with Customer Data Deletion timelines outlined in the table below.

Physical media on which Customer Data is stored during the contract term is not removed from the data centers that Salesforce uses to host Customer Data unless the media is at the end of its useful life or being de-provisioned, in which case the media is first sanitized before removal. This process is subject to applicable legal requirements.

Without limiting the ability for customers to request return of their Customer Data submitted to the Covered Services, Salesforce reserves the right to reduce the number of days it retains such data after contract termination. Salesforce will update its Salesforce Security, Privacy, and Architecture Documentation in the event of such a change.

Subscription Terminates Day 0 – 30	Day 30 – 120	Day 121 – 211	Day 121 – 301
Data available for return to customer	Data inactive and no longer available	Data deleted or overwritten from production	Data deleted or overwritten from backups

Customer Control Responsibilities and Considerations

This section describes additional customer control responsibilities and considerations. While these are not necessary for Salesforce Services' Covered Services to achieve its service commitments and system requirements, the following customer control considerations should be considered by user entities to further address their own commitments and system requirements.

Controls Customer Should Consider Implementing
Customers are responsible for configuring their implementation of the Covered Services, including security measures such as dedicated/specified IP addresses and multi-factor authentication. Where applicable, customers are responsible for the configuration of the user organization API system level calls to access Salesforce's API. Customers should reference the Salesforce Security Implementation Guide.
Customers are responsible for managing their organization's instance(s) of the Lightning Platform (formerly Force.com), installed applications as well as establishing any customized security solutions or automated processes through the use of setup features, application development tools, and API integration tools.
Customers are responsible for ensuring that authorized users are appointed as organizational administrators for granting access to the Covered Services' system.
Customers are responsible for notifying Salesforce of any unauthorized use of any password or account, or any other known or suspected breach of security related to the use of the Covered Services' system.
Customers are responsible for data classification and the implementation of encryption features available within the platform, where deemed necessary by customer-defined requirements.
Customers are responsible for managing and reviewing access of any user account such as Salesforce Customer Support, Professional Services, or other users providing assistance with covered services or applications.
Customers are responsible for reviewing activity logs of actions performed by Salesforce customer support, professional services, or other Salesforce teams providing assistance with covered services or applications.
Customers are responsible for any changes made to user organization data stored within the Covered Services' system.
Customers are responsible for customer code or functionality designed, developed, and deployed on the platform.

Controls Customer Should Consider Implementing
Customers are responsible for communicating relevant security, availability, and confidentiality issues and incidents to Salesforce through identified channels.
Customers are responsible for conducting periodic exports of data to meet their specific data retention requirements.
Customers are responsible for configuring the expiration of mobile refresh tokens.
Customers are responsible for the creating, editing and deleting reports using the report building tools and for ensuring the parameters for reports created by their personnel are relevant and accurate for the intended business needs.

Complementary Subservice Organization Controls

Salesforce Services' Covered Services relies on controls performed by Salesforce, Inc. Salesforce Corporate Services controls are performed and monitored by integrated Salesforce functions, and are not included in the scope of this report but are required to achieve the specified criteria. This report should be read in conjunction with the report issued by Salesforce, Inc. over the Salesforce Corporate Services Covered Services.

The Covered Services utilize public cloud providers to provide cloud infrastructure as mentioned above in the Locations and Infrastructure table. The public cloud providers are responsible for operating, managing, and controlling the underlying infrastructure components supporting the services which are utilized by Salesforce. Salesforce compliance teams review audit reports performed by independent auditors of the public cloud providers for security, availability, and confidentiality considerations.

Salesforce Services' Covered Services utilize Heroku Services for Certain Services. Refer to the Infrastructure & Sub-processors (I&S) documentation linked within the Salesforce Services Security, Privacy, and Architecture (SPARC) documentation for the Covered Services utilizing Heroku as a Sub-processor. This report should be read in conjunction with the report issued by Salesforce, Inc. over the Heroku Covered Services.

The following tables identify the impacted criteria and the complementary subservice organization controls (CSOCs) expected to be implemented at the Subservice Organizations as documented in the Service specific SOC reports in order to achieve the specified criteria, where applicable, based on the nature of the service:

Controls Expected to be Implemented at Salesforce Corporate Services

Controls Expected to be Implemented at Salesforce Corporate Services	Complemented Criteria
• Commitment to integrity and ethical values is established through management and communication of the Code of Conduct, employee background screenings and performance evaluations, and enforcement of disciplinary actions for non-compliance with Company policies and standards.	CC1.1

Controls Expected to be Implemented at Salesforce Corporate Services	Complemented Criteria
• BOD independence and oversight over internal controls is established in the BOD charter and through regular communications to the BOD.	CC1.2
• Company organizational structure and employee responsibilities are established within the Company's technology strategy, information security requirements and implementation plans, job descriptions and reporting lines, and the segregation of duties for job functions.	CC1.3
• Company personnel development, retention, and competency is managed through employee and contractor screening, the documented Information Security Policy and underlying security standards, ongoing security awareness and job specific trainings, and documented employee goals and the periodic evaluation of progress towards achieving goals.	CC1.4
• Accountability for an individual's internal control responsibilities is established through implementing and managing Company policies and standards, conducting periodic employee evaluations, and taking disciplinary action for information security non-compliance.	CC1.5
• The Company obtains, generates, and uses information from policies and standards, monitoring tools, and control and risk assessments to support the functioning of internal controls.	CC2.1
• The Company has established channels to communicate internally its security policies and standards, employee responsibilities and goals, training requirements, and methods for reporting incidents.	CC2.2
• The Company has established channels to communicate to external users its commitments related to security, availability, and confidentiality, and methods for users to report incidents.	CC2.3
• Trust sites are updated with advisories about security issues impacting customers.	CC2.3, CC7.4, CC7.5
• The Company has implemented security compliance audits, Business Continuity Program, BIA, Global Crisis Management Team Plan, incident response process, Vendor Management Program, anti-fraud program, and enterprise and security risk assessments to enable the identification and assessment of risks, including those arising from potential business disruptions and associations with vendors and business partners.	CC3.1, CC3.2, CC3.3, CC3.4, CC9.1, CC9.2, A1.1, A1.3, C1.1
• The Company performs activities, such as compliance audits, to assess whether internal controls are present and functioning.	CC4.1
• Identified internal control deficiencies are managed, tracked, communicated and remediated as required.	CC4.2

Controls Expected to be Implemented at Salesforce Corporate Services	Complemented Criteria
• The Company has documented security policies, continuity programs, incident response programs, risk management functions, and technology strategies to contribute to the mitigation of risks and support the achievement of objectives.	CC5.1, CC5.2
• Policies and standards that define control activities are documented, communicated, and reviewed periodically.	CC5.3
• The Company has implemented logical security tools and technologies to protect against security events and other threats from outside the boundaries of the system boundaries, such as a corporate VPN to access the corporate network, a security information and event management solution, and a TLS certificate monitoring and management tool.	CC6.1, CC6.6
• The Company manages authentication into the corporate network, and revokes user access to the corporate network in a timely manner upon termination.	CC6.2, CC6.3
• The Company reviews public cloud service provider audit reports performed by independent auditors to ensure appropriate physical access and environmental controls have been properly designed and implemented, and are operating effectively. • Data center hosting providers and sub-processors are evaluated by the Vendor Audit Program (VAP) prior to processing Customer Data. • The Vendor Audit Program (VAP) team performs annual supplier due-diligence reviews for all Tier 1 suppliers to monitor compliance with Salesforce security requirements. Any issues identified are evaluated and remediated in a timely manner.	CC6.4, CC6.5, A1.2
• The Company has implemented employee endpoint management solutions, such as mobile device management policies, laptop disk encryption monitoring, anti-malware protections, and software allowlisting tools.	CC6.7, CC6.8
• The Company has implemented a threat and vulnerability management program to identify and respond to vulnerabilities.	CC7.1, CC7.2
• The Company has a centralized team to track and resolve security issues identified in the products and services.	CC6.8, CC7.1
• The Company has implemented a security information and event management solution to monitor system components for security incidents. Logs are protected from tampering and retained for 1 year to support investigations into suspected security incidents.	CC7.2, CC7.3, CC7.4, CC7.5
• The Company has a customer support function for escalating and resolving incoming customer cases.	CC7.3, CC7.4

Controls Expected to be Implemented at Salesforce Corporate Services	Complemented Criteria
• CSIRT has defined processes to evaluate, escalate, track and resolve identified security incidents.	CC7.3, CC7.4, CC7.5
• The Company maintains a Change Management Standard which defines the requirements for performing changes, and is reviewed annually.	CC8.1
• The Company has a defined Data Classification Standard, which specifies classification levels and control requirements in order to meet the Company's commitments related to confidentiality.	C1.1

Controls Expected to be Implemented at other Salesforce Services Subservice Organizations

Controls Expected to be Implemented at AWS	Complemented Criteria
• Password and/or MFA is used to restrict access to authorized individuals. • Encryption methods are used to protect data in transit and at-rest. • Roles and responsibilities for managing cryptographic keys are formally documented. • Firewall devices are configured to restrict access to the computing environment and enforce boundaries of computing clusters. • Network communications within a VPN Gateway are isolated from network communications within other VPN Gateways. • Security protections are in place to restrict access to virtual and physical devices and other information assets to authorized personnel.	CC6.1
• Additions and changes to the system are authorized prior to access being granted. • System access is removed timely upon termination.	CC6.2
• System access is removed timely upon termination. • System access is reviewed on a periodic basis to ensure access is restricted to authorized and appropriate individuals. • IT access above least privileged, including administrator access, is approved by appropriate personnel prior to access provisioning.	CC6.3

Controls Expected to be Implemented at AWS	Complemented Criteria
• Only authorized personnel have access to the facilities housing the system. • Badge access control systems are in place in order to access the facilities. • Visitor access to the corporate facility and data center are recorded in visitor access logs. • Visitors are required to wear a visitor badge while onsite at the facilities. • Visitors are required to check in with security and show a government issued ID prior to being granted access to the facilities. • Visitors are required to have an escort at all times.	CC6.4
• Production media is securely decommissioned and physically destroyed prior to leaving the data center.	CC6.5
• External vulnerability assessments are performed on a periodic basis, identified issues are investigated and tracked to resolution in a timely manner.	CC7.1
• Changes are authorized, tested, and approved prior to implementation.	CC8.1
• Environmental protections have been installed including the following: – Cooling systems – Battery and generator backups – Smoke detection – Dry pipe sprinklers • Environmental protection equipment receives maintenance on at least an annual basis.	A1.2
• Backups of critical system components are monitored for successful replication across multiple data centers.	A1.3

Controls Expected to be Implemented at Heroku Services	Complemented Criteria
• Password and/or MFA is used to restrict access to authorized individuals. • Encryption methods are used to protect data in transit and at-rest. • Firewall devices are configured to restrict access to the computing environment and enforce boundaries of computing clusters. • Network communications within a VPN Gateway are isolated from network communications within other VPN Gateways. • Security protections are in place to restrict access to virtual and physical devices and other information assets to authorized personnel.	CC6.1

Controls Expected to be Implemented at Heroku Services	Complemented Criteria
• Additions and changes to the system are authorized prior to access being granted. • System access is removed timely upon termination.	CC6.2
• System access is removed timely upon termination. • System access is reviewed on a periodic basis to ensure access is restricted to authorized and appropriate individuals. • IT access above least privileged, including administrator access, is approved by appropriate personnel prior to access provisioning.	CC6.3
• The Disaster Recovery Plan outlines the actions to be followed to meet availability and system requirements, and is tested annually.	CC7.4, CC7.5, CC9.1, A1.2, A1.3
• Production systems are monitored for availability and capacity. Performance incidents are tracked, remediated, and communicated to external parties when customer impact.	CC9.1, A1.1
• Data is replicated between sites to support high availability.	CC9.1, A1.2
• Changes are authorized, tested, and approved prior to implementation.	CC8.1
• Backups of critical system components are monitored for successful replication across multiple data centers.	A1.3

Trust Services Criteria and Related Controls

Salesforce's criteria and related controls are included in Section IV of this report, "Salesforce, Inc.'s Criteria, Related Controls, and EY's Test Procedures and Results." Although the criteria, and related controls are presented in Section IV, they are an integral part of Salesforce, Inc.'s description of the Salesforce Services' Covered Services system as described in Section III.

Section IV: Salesforce, Inc.’s Criteria, Related Controls, and EY’s Test Procedures and Results

Security, Availability, and Confidentiality Criteria, Related Controls, and EY's Test Procedures and Results

Purpose and Context

On the following pages, the security, availability, and confidentiality criteria and the related control activities have been specified by, and are the responsibility of salesforce and are considered part of Management's description. EY's test procedures and EY's test results are the responsibility of the service auditor.

Trust Criteria and Related Controls for Systems and Applications

Content	Description
Criteria	The criteria represent the individual requirements for the in-scope categories of Security, Availability, and Confidentiality within the Trust Service Criteria issued by the AICPA. **Security Criteria** Information systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise its information or systems and affect the entity's ability to meet its service commitments and system requirements. **Availability Criteria** Information and systems are available for operation and use to meet the entity's service commitments and system requirements. **Confidentiality Criteria** Information designated as confidential is protected to meet the entity's service commitments and system requirements
Controls	The controls listed on the following pages depict Salesforce, Inc.'s controls which are related to the applicable criterion for Security, Availability, and Confidentiality. In addition to these controls, certain Complementary Subservice Organization Controls (CSOCs) expected to be implemented by Salesforce Corporate Services, Heroku Services, and AWS, which are defined Section III, are required to achieve the applicable criterion for Security, Availability, and Confidentiality. The Salesforce Corporate Services, Heroku Services, and AWS SOC reports should be read in conjunction with the Salesforce Services Covered Services system report.

Procedures Performed for Assessing the Completeness and Accuracy of Information Provided by the Entity

For tests of controls requiring the use of Information Produced by the Entity (IPE) (e.g., controls requiring system-generated populations for sample-based testing), EY performed a combination of the following procedures where possible based on the nature of the IPE to assess the completeness and accuracy of the IPE.

1. Inspected the source of the IPE
2. Inspected the query or script, and associated parameters used to generate the IPE from the source system
3. Reconciled IPE back to the source system of the IPE
4. Inspected the IPE for anomalous gaps in sequence or timing to determine the data is complete and accurate

In addition to the above procedures, for tests of controls which required management's use of IPE in the performance of controls (e.g., quarterly access reviews), where relevant, EY inspected the procedures performed by management to assess the completeness and accuracy of the IPE used in the performance of the control.

Controls, Criteria, Tests, and Results of Tests

Control Description	SOC 2 Criteria Reference	EY's Test Procedures	EY's Test Results
AC-05: Appropriate identification and authentication including multi-factor authentication (MFA) with dynamic password generation or password parameters set in accordance with corporate policy as system functionality allows are required to access the production systems.	CC6.1, CC6.2, CC6.3, CC7.1	Inspected authentication policy documentation to determine requirements for appropriate identification and authentication credentials, including multi-factor authentication, were defined.	No exceptions noted.
		Inspected system configurations for the production infrastructure to determine systems were configured to enforce multi-factor authentication with dynamic password generation or password parameters set in accordance with company policy as systems allow.	No exceptions noted.
		Observed a user traverse the authentication points required to gain logical access to the production infrastructure to determine appropriate identification and authentication credentials, including multi-factor authentication, were required to perform actions on the production infrastructure.	No exceptions noted.
AC-07: Secure encryption algorithms are used to remotely manage production infrastructure.	CC6.7, CC6.8	Observed an administrator log on to each remote access authentication path and inspected the configuration for each path to determine secure encryption algorithms were used when users remotely managed production infrastructure.	No exceptions noted.

Control Description	SOC 2 Criteria Reference	EY's Test Procedures	EY's Test Results
AC-13a: Access privileges are approved by management and documented prior to provisioning or access is granted by default based on the user's job function.	CC6.1, CC6.2, CC6.3	Inspected access policies and procedures to determine requirements for management approval and documentation of access creation were defined.	No exceptions noted.
		Inspected ticket details for a sample of production account creations and modifications, selected from the system access lists, to determine the access creation or modification was authorized by management and was documented.	No exceptions noted.
		Inspected system configurations with the ILM tool to determine approvals from the user's manager were systematically enforced for onboarded entitlements prior to the access being granted.	No exceptions noted.
		Inspected the ILM record for a sample user granted access to the system to determine the approval was obtained from the user's manager prior to automated provisioning and the access granted matched the access approved.	No exceptions noted.

Control Description	SOC 2 Criteria Reference	EY's Test Procedures	EY's Test Results
AC-13b: Pre-defined access roles and permissions are applied to public cloud environments upon creation.	CC6.1, CC6.2, CC6.3	Inspected the Public Cloud Security Standard to determine security control requirements for cloud service providers were defined.	No exceptions noted.
		Inspected read-only role permissions to determine it did not include any privileged access.	No exceptions noted.
		Inspected configurations that applied permission boundaries to AWS accounts to determine IAM policies were enforced based on Salesforce standards.	No exceptions noted.
		Inspected system configurations within the code repository to determine permission boundary rules were enforced for all public cloud role creations to prevent creation of new users and roles without permission boundary, and prevent any role from having permissions to modify or delete permission boundary rules and from creating login profiles that could access the system outside of PCSK.	No exceptions noted.
		Observed a user attempt to create a new user and role without permissions boundary and determined the system prevented the actions.	No exceptions noted.
		Observed a user attempt to modify the boundary permissions of a role, and create a login profile outside of PSCK to determine the system prevented the actions.	No exceptions noted.

Control Description	SOC 2 Criteria Reference	EY's Test Procedures	EY's Test Results
AC-14: Production user access is revoked timely following the creation of a termination case in accordance with Salesforce Security Standards.	CC6.1, CC6.2, CC6.3	Inspected the Access Management standard and supporting documented procedures to determine the guidelines and boundaries of the access termination process were identified, and that the standard was reviewed annually.	No exceptions noted.
		Inspected termination automation configurations to determine user accounts were automatically disabled/terminated when a termination case was created and alerts were generated in the event of a failure.	Management made us aware of potential delays in terminations due to employment record data flows and processing errors with ILM automation. Management has designed AC-40 to identify any failures in execution of automation and corporate network access termination processes, as noted in the Corporate Services SOC report, for timely removal of AD/SSO access which would prevent access to downstream systems. No other exceptions noted.
		Inspected details for a sample of termination automation failures, selected from the notification channel, to determine the issues were resolved and the user's access was removed timely.	No exceptions noted.

Control Description	SOC 2 Criteria Reference	EY's Test Procedures	EY's Test Results
		Inspected termination tickets for a sample of GIA and Mobile Publisher terminated employees who were not subject to the automated termination process, selected from the system access lists and HR termination reports to determine access was revoked in a timely manner following termination.	For the one (1) terminated user with access to Mobile Publisher within the examination period, user's access was not revoked timely in accordance with the Salesforce Security Standard.
Management response: Salesforce management internally identified, investigated, and notified the auditors of the late access deprovisioning in Mobile Publisher in accordance with Salesforce Security Standard. Salesforce management identified that the user was assigned read-only access to objects with limited reporting permission. Furthermore, Salesforce management confirmed that the user did not access the system after the termination date. Mobile Publisher Quarterly Access Review (QAR) operated effectively as a compensating control during the examination period.			
AC-15: Internal Admin Portal user access is revoked timely following the creation of a termination case in accordance with Salesforce Security Standard.	CC6.1, CC6.2, CC6.3	Inspected the Access Management standard to determine the user termination requirements were defined.	No exceptions noted.
		Inspected termination tickets for a sample of terminated employees and contractors selected from the system access lists and HR termination reports to determine their access to the Internal Admin Portal was revoked in a timely manner (within five (5) business days and/or within one (1) business day for the Government Cloud environment) following termination.	For one (1) of the twenty-five (25) terminated users with access to the Standard Internal Admin Portal, the user's access was not revoked timely in accordance with the Salesforce Security Standard.
Management Response: Salesforce management acknowledges that one terminated Standard Internal Admin Portal user account was not deactivated timely during a transition between control performers. The risk due to the access is limited as the Standard Internal Admin Portal requires Salesforce Corporate credential access, which was terminated timely for the user in accordance with the Salesforce Security Standard. Salesforce management reviewed the last login date within the Standard Internal Admin Portal for the user account and determined that there was no access after the termination date.			

Control Description	SOC 2 Criteria Reference	EY's Test Procedures	EY's Test Results
AC-17: Production user access is reviewed for role changes and transfers. Issues identified are investigated and resolved within 30 days of transfer.	CC5.2, CC5.3, CC6.2, CC6.3	Inspected the Logical Access Management Standard to determine requirements for reviewing Salesforce Services production access on a monthly basis for role changes and transfers were defined.	No exceptions noted.
		Inspected system configurations to determine a transfer review ticket was systematically created in the event of a role change or transfer, and access is automatically revoked once the transfer tickets did not obtain approval.	No exceptions noted.
		Inspected the transfer review ticket details for a sample of tickets selected from the ticketing system to determine the review was completed for role changes and transfers, and any issues identified were investigated and resolved within 30 days of the role change or transfer.	No exceptions noted.
AC-18: Production network and server user access is reviewed on a quarterly basis. Accounts identified as not being appropriate are investigated and resolved.	CC6.2	Inspected Access Management standard to determine requirements and guidance to perform user access reviews were documented.	No exceptions noted.
		Inspected quarterly access review ticket details for a sample quarter to determine the quarterly access review of user accounts were performed, and any accounts identified for removal were investigated and resolved.	No exceptions noted.

Control Description	SOC 2 Criteria Reference	EY's Test Procedures	EY's Test Results
AC-19: Production database user accounts are reviewed on a quarterly basis. Accounts identified as not being appropriate are investigated and resolved.	CC6.2	Inspected the Logical Access Management standard to determine requirements for access reviews were defined.	No exceptions noted.
		Inspected quarterly access review ticket details for a sample quarter to determine quarterly access reviews of database access were performed, and any issues identified were investigated and resolved.	No exceptions noted.
AC-20: Internal Admin Portal logical access is reviewed on a quarterly basis. Accounts identified as not being appropriate are investigated and resolved.	CC6.2	Inspected the access review documentation for a sample quarter to determine that Internal Admin Portal user accounts were reviewed by management quarterly and accounts identified as inappropriate were investigated and resolved.	No exceptions noted.
AC-22a: Vendor provided database accounts are locked, removed or the default password is changed.	CC6.2, CC6.6	Inspected Salesforce's Oracle Hardening Guide to determine vendor provided (default) database account passwords were required to be locked, or removed, or the default password was required to be changed for accounts that were not needed or being used.	No exceptions noted.
		Inspected vendor provided (default) database accounts on a sample of production PODS selected from trust site to determine accounts which were not needed or used, were locked or removed, or the default password was changed.	No exceptions noted.
AC-22b: The Management console root account password is stored in a password vault where access is restricted to a limited number of authorized personnel.	CC6.2, CC6.6	Inspected the job title, reporting chain, and performed inquiry of the control owner for the list of users who have access to the password vault to determine access was restricted to a limited number of authorized personnel.	No exceptions noted.

Control Description	SOC 2 Criteria Reference	EY's Test Procedures	EY's Test Results
AC-24: Customer users of the system are uniquely identified and authenticated. Customers cannot access the application without a valid user ID and password.	CC6.1, CC6.2	Inspected the application login page to determine that customers could not access the application without a valid user ID and password that was provided when the customer signed up for the service.	No exceptions noted.
		Observed a new user sign-up as a customer to determine valid user credentials must be provided as part of the sign-up procedure.	No exceptions noted.
		Observed a user attempt to access the services using invalid login credentials to determine access was denied.	No exceptions noted.
AC-29: Support personnel do not have access to log in as a customer unless authorized by the customer. Customers grant access for troubleshooting purposes and define the duration of the access.	CC5.2, CC6.1, CC6.2, CC6.3	Inspected Salesforce's Grant Login Access support article to determine the procedures for granting login access to Salesforce Support personnel were documented.	No exceptions noted.
		Observed a system administrator attempt to access customer data on a demo customer account prior to being granted access to determine access to the customer accounts was not available.	No exceptions noted.
		Observed a system administrator on a demo customer account grant login access for Salesforce Support to determine customer authorization was required along with the specified systematically enforced duration of access availability.	No exceptions noted.

Control Description	SOC 2 Criteria Reference	EY's Test Procedures	EY's Test Results
		Observed a Salesforce Support individual access the demo customer account through the application to determine the individual was logged in as the system administrator on the demo customer account and access was removed after the defined duration.	No exceptions noted.
		Inspected system configurations within the code repository to determine that login access granted to Support personnel is revoked based on the defined duration set by the customer.	No exceptions noted.
AC-32: On a semi-annual basis, management performs a review of access provisioned via automation by identity lifecycle management tools to validate that access requests are approved and access is granted in accordance with Salesforce Security Standards.	CC6.1, CC6.2, CC6.3	Inspected the semi-annual access review testing workpaper and supporting evidence to determine the access review of user accounts was performed, and any inappropriate access was investigated and resolved.	No exceptions noted.
AC-39: ILM tools monitor for access data discrepancies between ILM tool access record databases and production systems. Identified discrepancies are investigated and remediated.	CC6.3	Inspected system configurations within ILM to determine a comparison was performed between the ILM tool access record databases and the target production system on a daily basis and created a Divergence Case for any discrepancy.	No exceptions noted.
		Inspected the Divergence Case details and supporting evidence for a sample of cases selected from the ticketing system to determine the discrepancies were investigated and resolved timely.	No exceptions noted.

Control Description	SOC 2 Criteria Reference	EY's Test Procedures	EY's Test Results
AC-40: A quarterly analysis is performed to detect Termination and Transfers events not successfully triggered in the Identity Lifecycle Management tools. Identified events are investigated and resolved in accordance to the expected service-level agreement.	CC6.3	Inspected the quarterly analysis details for a sample quarter to determine a review Termination and Transfer event failures was performed, and issues identified were investigated and resolved.	While the review was performed, the sampled review was performed 19 days after the required timeline.
Management Response: Salesforce management adjusted internal review requirements to align with the existing quarterly user access review timeliness requirements.			
AU-02a: Production network devices, databases and servers are configured to log privileged operations, authorized access, and unauthorized access attempts.	CC2.1, CC5.2, CC7.2	Inspected the logging and monitoring policy document to determine logging and auditing requirements, including activities of privileged users, were defined.	No exceptions noted.
		Inspected the baseline configurations applied to production instances to determine they were configured to log privileged operations, authorized access, and unauthorized access attempts.	No exceptions noted.
		Inspected configurations for a sample of network devices and databases selected from the asset inventory to determine they were configured to log privileged operations, authorized and unauthorized access attempts.	No exceptions noted.
		Inspected configurations for one sample server selected from the asset inventory to determine if it was configured to log privileged operations, authorized and unauthorized access attempts per the configuration management tool.	No exceptions noted.

Control Description	SOC 2 Criteria Reference	EY's Test Procedures	EY's Test Results
		Observed an authentication event on a sample asset and inspected the corresponding details within the centralized logging system to determine the events were logged	No exceptions noted.
		Observed a privileged event and inspected the corresponding details within the centralized logging system to determine the event was logged.	No exceptions noted.
AU-02b: Production network device, database, and server logs are transmitted to a centralized logging system.	CC2.1, CC5.2, CC7.2	Inspected the baseline configurations applied to production instances to determine they were configured to transmit the logs to a centralized logging system.	No exceptions noted.
		Observed a successful and unsuccessful login attempt on a sample asset and inspected the corresponding details within the centralized logging system to determine the events were logged.	No exceptions noted.
		Observed a privileged event and inspected the corresponding details within the centralized logging system to determine the event was logged.	No exceptions noted.
AU-03: Clocks of relevant information processing systems are synchronized with a centralized Network Time Protocol (NTP) server at least hourly.	CC2.1, CC7.2	Inspected the configuration for a sample of GPS appliances selected from the asset inventory to determine the device was configured to use GPS satellites as the time source and had at least one associated NTP pool server configured to synchronize at least hourly.	No exceptions noted.

Control Description	SOC 2 Criteria Reference	EY's Test Procedures	EY's Test Results
		Inspected the NTP configuration within the configuration management tool to determine servers were configured to use NTP as the basis for clock synchronization.	No exceptions noted.
		Inspected the configuration for a sample of network devices and servers selected from the asset inventory to determine the device was configured to synchronize with NTP pool servers at least hourly.	No exceptions noted.
AU-05: Activities performed by support personnel using the login as functionality for a given customer are logged and available for customer review.	CC5.2	Observed a system administrator on a demo customer account grant login access for Salesforce Support to determine authorization was required.	No exceptions noted.
		Observed a Salesforce Support individual access the demo customer account through the application using the login as functionality and inspected the corresponding access logs to determine setup and metadata changes performed were logged and available for customer review.	No exceptions noted.
		Inspected the retention configuration to determine that audit trail logs containing the activities performed by support personnel using the login-as functionality were retained for 6 months.	No exceptions noted.
CM-01: Capacity planning is conducted so that necessary capacity for long term strategic planning exists.	CC4.1, CC7.5, A1.1	Inspected the POD demand schedule and Instance Requirement plan to determine long term capacity planning was performed at least annually.	No exceptions noted.

Control Description	SOC 2 Criteria Reference	EY's Test Procedures	EY's Test Results
		Inspected the calendar invite to determine that a recurring meeting was scheduled with Capacity Planning and Engineering team to discuss capacity addition prioritization.	No exceptions noted.
CM-02: A version management system is utilized to maintain current and prior configurations for production servers, network devices, and databases.	CC2.1, CC7.1, CC8.1	Inspected the version management system to determine current and prior configurations for production code configurations were maintained.	No exceptions noted.
CM-04: Application code changes are documented, tracked, and peer reviewed and/or approved by management.	CC2.1, CC5.2, CC5.3, CC6.8, CC8.1	Inspected Salesforce's Global Change Management Policy to determine requirements and procedures for changes made to production systems were defined.	No exceptions noted.
		Inspected the configurations of the code repository tools to determine application changes to production code were tracked via a ticket or a pull request.	No exceptions noted.
		Inspected details for a sample of application code changes selected from the ticketing system and the code repository to determine peer review was successfully completed prior to production release.	No exceptions noted.

Control Description	SOC 2 Criteria Reference	EY's Test Procedures	EY's Test Results
CM-05a: Infrastructure changes are documented, tracked, and peer reviewed and/or approved by management.	CC6.1, CC6.8, CC8.1	Inspected change management procedures documentation to determine approval requirements, and guidelines for assessing risk and impact of changes based on change type were documented.	No exceptions noted.
		Inspected the change details for a sample of infrastructure changes selected from the ticketing system to determine the change was peer reviewed and/or approved by management prior to implementation and was implemented by an individual separate from the approver.	No exceptions noted.
CM-05b: Standard Pre-Approved changes relate to low-risk recurring changes that utilize established pre-approved templates or are systematically implemented based on the pre-approved change category.	CC6.1, CC6.8, CC8.1	Inspected the implementation details for a sample of Standard Pre-Approved infrastructure change selected from the ticketing system to determine the changes were implemented using a standard pre-approved template or were systematically implemented based on the pre-approved change category.	No exceptions noted.
CM-06a: A change risk impact analysis is documented prior to implementing an infrastructure change, as necessary based on the nature of the change.	CC8.1	Inspected the change record details for a sample of the production infrastructure changes selected from the ticketing system to determine a change risk impact analysis was documented prior to implementing the infrastructure change, as necessary, based on the nature of the change.	No exceptions noted.
CM-06b: A roll-back plan is documented prior to implementing an infrastructure change, as necessary, based on the nature of the change.	CC8.1	Inspected the change record details for a sample of production infrastructure changes selected from the ticketing system to determine a roll-back plan was documented prior to implementing the infrastructure change, as necessary, based on the nature of the change.	No exceptions noted.

Control Description	SOC 2 Criteria Reference	EY's Test Procedures	EY's Test Results
CM-07: Access to deploy application changes to production environments is restricted to authorized personnel.	CC6.8, CC8.1	Inspected the job title, reporting chain, and performed inquiry of the control owner for users with access to deploy changes to production environments, obtained from the system access lists, to determine access to make changes to production environments was restricted to authorized personnel.	No exceptions noted.
CM-08: A current asset inventory of production systems is documented and maintained.	CC3.2, CC6.1, CC7.1	Inspected the Annual Asset Inventory procedures to determine requirements for an annual asset inventory were defined.	No exceptions noted.
		Inspected the ticket details for the most recent annual asset inventory review for a sample of data centers selected from the Vendor Audit Program team tracking list to determine an annual asset inventory check was performed to maintain the system inventory, and the review included active devices in the production network within the past year.	No exceptions noted.
CM-09: Documented configuration guidelines for the production environment govern the configuration management process.	CC2.1, CC6.8, CC7.1, CC8.1	Inspected the configuration standard and supporting documents to determine configuration guidelines for the production environment existed which governed the configuration management process.	No exceptions noted.
CM-13: A centralized management tool is utilized to configure and manage production infrastructure.	CC6.8, CC7.1	Inspected the centralized configuration management tool configurations to determine it was configured to check in with the hosts periodically and automatically update hosts to the approved system baseline.	No exceptions noted.
		Inspected the production host build script configurations to determine the configuration management agent was installed as part of the build process.	No exceptions noted.

Control Description	SOC 2 Criteria Reference	EY's Test Procedures	EY's Test Results
		Inspected configurations for a sample of production hosts selected from the asset inventory to determine the centralized configuration management agent was installed.	No exceptions noted.
		Observed a user make a change directly on an example production host to determine after the specified period of time, the configuration management system automatically updated the host to the approved baseline.	No exceptions noted.
		Inspected the network device configuration management tool to determine it existed to support the initiation and set up of network devices using pre-defined baseline configuration.	No exceptions noted.
		Inspected the database configuration management tool to determine that changes to database configurations that are not within the baseline configurations resulted in alert for investigation.	No exceptions noted.
CP-01: The Disaster Recovery Plan (DRP) outlines the actions to be followed to meet availability and system requirements. The DRP is reviewed annually by relevant stakeholders.	CC7.4, CC7.5, CC9.1, A1.2	Inspected the Disaster Recovery Plan to determine it outlined the actions to be followed in the event of a disaster to bring the production systems back online to meet availability and system requirements and the plan was reviewed within the past year.	No exceptions noted.
CP-04: Contingency documentation is communicated to individuals with contingency roles and responsibilities.	CC1.4, CC2.2, CC7.5, CC9.1	Inspected Salesforce's Site Reliability Intranet site to determine Site Reliability playbooks existed and contained contingency documentation, including roles and responsibilities, escalation paths, and site switch process details.	No exceptions noted.

Control Description	SOC 2 Criteria Reference	EY's Test Procedures	EY's Test Results
CP-05: A disaster recovery plan is tested at least annually to determine the effectiveness of the plan. The results of testing are reviewed and corrective action is taken as necessary.	CC7.5, CC9.1, A1.2, A1.3	Inspected Salesforce's Infrastructure Engineering Disaster Recovery Plan to determine annual disaster recovery activities were required to test the established Recovery Time Objective (RTO), Recovery Point Objective (RPO), and failover to alternate processing sites.	No exceptions noted.
		Inspected the site switch schedule to determine a schedule for failover testing was defined.	No exceptions noted.
		Inspected the results of the most recent instance of a disaster recovery test to determine effectiveness of the plan was tested within the past year, and results were reviewed and corrective actions required were documented as necessary.	No exceptions noted.
CP-06: The Salesforce Private Connect AWS environment is configured for high availability across multiple availability zones.	CC7.5, CC9.1, A1.2, A1.3	Inspected system configurations of Private Connect to determine the production systems were configured for high availability across multiple availability zones.	No exceptions noted.
CP-07: Production systems are monitored for availability and capacity. Performance incidents are documented in a ticketing system.	CC9.1, A1.1	Inspected the monitoring configuration in the centralized configuration management tool to determine hosts were monitored for availability and capacity.	No exceptions noted.
		Inspected the monitoring dashboard to determine production systems were monitored for availability and capacity.	No exceptions noted.
		Inspected the on-call monitoring schedule to determine on-call personnel were assigned for responding to alerts.	No exceptions noted.

Control Description	SOC 2 Criteria Reference	EY's Test Procedures	EY's Test Results
		Inspected incident details for a sample of performance incidents selected from the incident management system to determine the incident was documented and tracked to resolution.	No exceptions noted.
CP-09: Primary and secondary storage/processing sites are geographically separated. Data is replicated between sites to support high availability.	CC9.1, A1.2	Inspected database replication configurations for a sample of production and sandbox instances selected from the trust site to determine the systems were configured to replicate data between geographically separate primary and secondary storage sites.	No exceptions noted.
		Inspected replication monitoring configurations to determine criteria was defined to generate alerts for database replication lag or failures.	No exceptions noted.
CP-12: Database backups are performed and retained in accordance with the defined schedule in the backup procedures.	CC9.1, A1.2, C1.1	Inspected policy documentation on the company's intranet to determine backup and retention requirements were defined.	No exceptions noted.
		Inspected the database backup schedule and associated backup scripts for a sample of PODS selected from the Salesforce Trust website to determine backups were configured in accordance with the defined schedule and retention requirements.	No exceptions noted.
CP-13: Production data in Fileforce servers is replicated near real time from the primary site to a secondary site.	CC9.1, A1.2	Inspected the Fileforce replication configurations to determine Fileforce servers were configured to replicate production data from the primary site to the secondary site in near real time.	No exceptions noted.

Control Description	SOC 2 Criteria Reference	EY's Test Procedures	EY's Test Results
		Observed a user upload a file attachment to determine it was saved to the Primary Fileforce site and replicated to the secondary site in near real-time.	No exceptions noted.
		Inspected the Fileforce replication status for a sample of PODS selected from the Salesforce Trust website to determine production data in Fileforce servers was successfully replicated from the primary site to a secondary site.	No exceptions noted.
IA-02a: Server, network device, and database accounts are automatically disabled once passwords expire and a new password is not set.	CC6.1	Inspected server, network device and database authentication system configurations to determine user accounts were configured to automatically disable once passwords expired and if a new password was not set.	No exceptions noted.
IA-02b: User access to the public cloud service provider administrative console and production infrastructure is provided on an as needed basis utilizing ephemeral credentials valid for only that purpose and time of use, and requires documented approval prior to being granted access.	CC6.1	Inspected configurations within the management console to determine access to the public cloud provider administrative console and production infrastructure was restricted to a defined period of time.	No exceptions noted.
		Observed a user attempt to submit an access request to determine the user could not approve their own access request, a reason for the access request was required, and approval was required prior to the access being granted for the configured duration.	No exceptions noted.
		Inspected the account status details for an example user account to determine the access was removed after the configured duration for the access has expired.	No exceptions noted.

Control Description	SOC 2 Criteria Reference	EY's Test Procedures	EY's Test Results
IR-03: Incident handling capabilities for performance incidents have been implemented. Customer impacting performance incidents are assigned a severity level to prioritize their importance.	CC2.1, CC5.1, CC5.3, CC7.4, CC7.5, CC8.1, CC9.1	Inspected Incident Response documentation to determine requirements and procedures for handling performance incidents were defined, including assignment of severity levels to prioritize their importance.	No exceptions noted.
		Inspected ticket details for a sample of customer impacting performance incidents selected from the ticketing system to determine the incidents were documented and assigned a severity level to prioritize their importance.	No exceptions noted.
IR-04: Investigation and corrective actions for customer impacting performance incidents are documented and shared with key personnel.	CC5.1, CC5.2, CC7.3, CC7.4, CC7.5, CC9.1	Inspected ticket details for a sample of customer impacting performance incidents selected from the ticketing system to determine investigation and corrective actions were documented and shared with key personnel.	No exceptions noted.
RA-06: Annually, Salesforce products complete infrastructure penetration testing for in-scope systems. Remediation of results are tracked to resolution.	CC4.1	Inspected Salesforce's Vulnerability Scanning and Penetration Testing Standard and Identification Process and Vulnerability Rankings Standard to determine requirements for the performance of penetration testing on an annual basis and the vulnerability ranking standards were defined.	No exceptions noted.
		Inspected the most recent penetration test results to determine that the test was performed within the past year and issues identified were tracked to resolution.	No exceptions noted.
SA-01: Code versioning software is used during the Salesforce Secure Development Lifecycle and supports rollback.	CC8.1	Inspected the code versioning software to determine it was used during the systems development life cycle and could support roll-back if necessary.	No exceptions noted.

Control Description	SOC 2 Criteria Reference	EY's Test Procedures	EY's Test Results
SA-03: Application releases into production do not occur until appropriate sign-offs are obtained and documented.	CC6.1, CC8.1	Inspected the ticket details for a sample of application releases into production, selected from the ticketing system, to determine appropriate sign-offs were obtained prior to release into production based on the release type.	No exceptions noted.
SA-10: Release notes are documented and communicated for every major release to users for changes and maintenance that affect system security, availability and confidentiality.	CC2.2, CC2.3, CC3.1, CC7.1	Inspected Salesforce's publicly available website to determine release notes were documented and communicated to users for changes and maintenance that affected system security, availability, and confidentiality.	No exceptions noted.
SC-02: Customers do not have direct access to the underlying back-end infrastructure to perform system management activities.	CC6.1	Inspected the organization chart records and access review documentation for a sample of users with access to the underlying back-end infrastructure, selected from the system access lists, to determine write access was restricted to Salesforce employees and was reviewed periodically for appropriateness.	No exceptions noted.
SC-03: Internal and external Domain Name Systems (DNS) are redundant and fault-tolerant.	A1.1, A1.2	Inspected the internal and external DNS configurations for the domain to determine they were redundant and fault tolerant.	No exceptions noted.
		Inspected the internal and external DNS configurations on a POD for a sample of in-scope production data centers to determine they were redundant and fault-tolerant.	No exceptions noted.

Control Description	SOC 2 Criteria Reference	EY's Test Procedures	EY's Test Results
SC-06: Production and non-production environments are segregated.	CC6.1, CC6.3, CC8.1	Inspected a network topology diagram to determine production networks were separated from the corporate and non-production environments.	No exceptions noted.
		Observed a user attempt to establish a connection between the non-production and production networks to determine the environments were separated to prohibit network access and information flow.	No exceptions noted.
SC-07: The application is designed to prevent customers from accessing the data of other customers.	CC6.1	Inspected architecture documentation to determine the application was designed to prevent a customer from accessing another customer's data.	No exceptions noted.
		Created two customer accounts and attempted to access each other's data and account to determine that the data and account information of the other customer were not accessible.	No exceptions noted.
SC-08: The production environment protects against or limits the effects of denial-of-service attacks.	A1.1	Inspected the DDoS protection service dashboard to determine traffic was routed through the DDoS protection service provider to protect against or limit the effect of denial-of-service attacks.	No exceptions noted.
		Inspected the service agreement between Salesforce and the third-party DDoS protection service provider to determine the agreement was in place to provide services to protect against or limit the effect of denial-of-service attacks.	No exceptions noted.

Control Description	SOC 2 Criteria Reference	EY's Test Procedures	EY's Test Results
		Inspected the Network Security DDoS Playbook within Confluence to determine high level incident handling workflows and escalation paths were defined to protect against or limit the effect of denial-of-service attacks.	No exceptions noted.
SC-09: Sessions into the production infrastructure (network, servers, and database) and the application are automatically terminated after a period of inactivity and requires reauthentication.	CC6.1	Inspected the authentication policy documentation to determine session setting timeout requirements were defined.	No exceptions noted.
		Inspected the secure virtual gateway configurations to determine they were configured to automatically terminate production sessions after a period of inactivity in accordance with policy.	No exceptions noted.
		Inspected the application configurations to determine it was configured to automatically terminate production sessions after a period of inactivity in accordance with policy.	No exceptions noted.
SC-10: Network traffic is protected and managed at external network connections by routing through boundary protection mechanisms.	CC6.1, CC6.6	Inspected network topology diagrams to determine boundary protection mechanisms were in place to manage inbound and outbound external connections.	No exceptions noted.
		Inspected the configuration for a sample of production firewall devices, selected from the asset inventory list to determine they were configured to deny all traffic by default, and a secure authentication protocol was enabled.	No exceptions noted.

Control Description	SOC 2 Criteria Reference	EY's Test Procedures	EY's Test Results
SC-11: Encryption is used to protect the confidentiality and integrity of information being transmitted over the Internet between the Customer and Salesforce.	CC6.1, CC6.6, CC6.7	Inspected policy documentation to determine encryption requirements were defined.	No exceptions noted.
		Inspected the certificate details for the services login pages to determine information transmitted over the Internet between the Customer and Salesforce was encrypted.	No exceptions noted.
SC-13: Customer data is encrypted based on the Customer's selection of platform encryption or field-level encryption.	CC6.1	Inspected Salesforce's encryption standards and procedures to determine it documented details of the encryption methods.	No exceptions noted.
		Inspected system configurations from the code repository to determine field data encryption was enforced based on customer specifications.	No exceptions noted.
		Inspected the data fields within a demo customer account to determine field level data was encrypted per selections made on the demo customer account.	No exceptions noted.
SC-14: Classic and Platform Cryptographic keys are rotated each major release in accordance with the Cryptographic Key Management Standard.	CC6.1	Inspected Salesforce's Cryptographic Key Management Standard to determine it documented the process on how encryption keys were managed and stored and requirements for the destruction of encryption keys.	No exceptions noted.
		Inspected Salesforce's classic and platform encryption configuration code to determine encryption keys were secured during transmission and storage.	No exceptions noted.

Control Description	SOC 2 Criteria Reference	EY's Test Procedures	EY's Test Results
		Inspected ticket details of Salesforce's encryption key signing ceremony for the most recent major release to determine encryption keys were generated in accordance with Salesforce's policies and standards.	No exceptions noted.
SI-08: Application code changes are tested prior to implementation into production.	CC8.1	Inspected details for a sample of application code changes selected from ticketing system and the code repository to determine testing was successfully completed prior to production release.	No exceptions noted.
SI-09a: Confidential customer data is disposed of per commitments defined in the customer agreements.	C1.2	Inspected the Main Subscription Agreement, and Trust and Compliance documentation on the Help site to determine commitments regarding the disposal of confidential Customer Data were communicated to customers.	No exceptions noted.
		Inspected the scripts used for the automated deletion of Customer Data from databases to determine the system was configured to delete customer confidential data in accordance with the defined commitments.	No exceptions noted.
		Inspected organization database records for a sample of organizations that were terminated, selected from the customer management system, to determine the data was deleted timely in accordance with the commitments.	For the period 5/1/2022 – 6/22/2022, data from Mobile Publisher Broker Org was not deleted until Management remediated the process on 6/22/2022. No deviations were noted from the period following 6/22/2022.

Control Description	SOC 2 Criteria Reference	EY's Test Procedures	EY's Test Results
Management Response: Salesforce internally identified, investigated, and notified the auditors of the data deletion issue impacting Mobile Publisher, which was remediated on June 22, 2022. Upon identification of the issue, Salesforce management implemented enhancements to the Mobile Publisher data deletion process to better align to Customer commitments and confirmed deletion was successfully executed for impacted attrited orgs. The data stored by Mobile Publisher is limited only to Customer "Branding Material" (such as brand names, logos, graphic assets, etc.) provided by the Customer to Salesforce to personalize the Salesforce Mobile application to match the Customer's branding and style preferences. Branding Material is a subset of Customer Data covered by the Salesforce Services SPARC and defined in the Salesforce Main Services Agreement. The Branding Material is shared publicly once the customized app is published to the Google Play Store and Apple App Stores on behalf of the Customer.			
SI-09b: Confidential customer data on Fileforce is disposed of per commitments defined in the customer agreements.	C1.2	Inspected the Main Subscription Agreement, and Trust and Compliance documentation on the Help site to determine commitments regarding the disposal of confidential Customer Data were communicated to customers.	No exceptions noted.
		Inspected the scripts used for the deletion of Customer Data from databases to determine the system was configured to delete customer confidential data in accordance with the defined commitments.	No exceptions noted.
		Inspected organization database records for a sample of organizations that were terminated, selected from the customer management system, to determine the data was deleted timely in accordance with the commitments.	No exceptions noted.

Criteria to Controls Mapping

Criteria	Controls List	Criteria
CC 1.0 Common Criteria Related to Control Environment		
CC1.1	Criteria addressed via subservice provider controls.	The entity demonstrates a commitment to integrity and ethical values.
CC1.2	Criteria addressed via subservice provider controls.	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
CC1.3	Criteria addressed via subservice provider controls.	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
CC1.4	CP-04 Criteria also addressed via subservice provider controls.	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
CC1.5	Criteria addressed via subservice provider controls.	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.
CC 2.0 Common Criteria Related to Communication and Information		
CC2.1	AU-02a, AU-02b, AU-03, CM-02, CM-04, CM-09, IR-03 Criteria also addressed via subservice provider controls.	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.
CC2.2	CP-04, SA-10 Criteria also addressed via subservice provider controls.	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
CC2.3	SA-10 Criteria also addressed via subservice provider controls.	The entity communicates with external parties regarding matters affecting the functioning of internal control.
CC 3.0 Common Criteria Related to Risk Assessment		
CC3.1	Criteria addressed via subservice provider controls.	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
CC3.2	CM-08 Criteria also addressed via subservice provider controls.	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.

Criteria	Controls List	Criteria
CC3.3	Criteria addressed via subservice provider controls.	The entity considers the potential for fraud in assessing risks to the achievement of objectives.
CC3.4	Criteria addressed via subservice provider controls.	The entity identifies and assesses changes that could significantly impact the system of internal control.
CC 4.0 Common Criteria Related to Monitoring Activities		
CC4.1	CM-01, RA-06 Criteria also addressed via subservice provider controls.	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
CC4.2	Criteria addressed via subservice provider controls.	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.
CC 5.0 Common Criteria Related to Control Activities		
CC5.1	IR-03, IR-04 Criteria also addressed via subservice provider controls.	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
CC5.2	AC-17, AC-29, AU-02a, AU-02b, AU-05, CM-04, IR-04 Criteria also addressed via subservice provider controls.	The entity also selects and develops general control activities over technology to support the achievement of objectives.
CC5.3	AC-17, CM-04, IR-03 Criteria also addressed via subservice provider controls.	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.
CC 6.0 Common Criteria Related to Logical and Physical Access Controls		
CC6.1	AC-05, AC-13a, AC-13b, AC-14, AC-15, AC-24, AC-29, AC-32, CM-05a, CM-05b, CM-08, IA-02a, IA-02b, SA-03, SC-02, SC-06, SC-07, SC-09, SC-10, SC-11, SC-13, SC-14 Criteria also addressed via subservice provider controls.	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.

Criteria	Controls List	Criteria
CC6.2	AC-05, AC-13a, AC-13b, AC-14, AC-15, AC-17, AC-18, AC-19, AC-20, AC-22a, AC-22b, AC-24, AC-29, AC-32 Criteria also addressed via subservice provider controls.	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
CC6.3	AC-05, AC-13a, AC-13b, AC-14, AC-15, AC-17, AC-29, AC-32, AC-39, AC-40, SC-06 Criteria also addressed via subservice provider controls.	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.
CC6.4	Criteria addressed via subservice provider controls.	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.
CC6.5	Criteria addressed via subservice provider controls.	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.
CC6.6	AC-22a, AC-22b, SC-10, SC-11 Criteria also addressed via subservice provider controls.	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.
CC6.7	AC-07, SC-11 Criteria also addressed via subservice provider controls.	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.
CC6.8	AC-07, CM-04, CM-05a, CM-05b, CM-07, CM-09, CM-13 Criteria also addressed via subservice provider controls.	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.

Criteria	Controls List	Criteria
CC 7.0 Common Criteria Related to System Operations		
CC7.1	AC-05, CM-02, CM-08, CM-09, CM-13, SA-10 Criteria also addressed via subservice provider controls.	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.
CC7.2	AU-02a, AU-02b, AU-03 Criteria also addressed via subservice provider controls.	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.
CC7.3	IR-04 Criteria also addressed via subservice provider controls.	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.
CC7.4	CP-01, IR-03, IR-04 Criteria also addressed via subservice provider controls.	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.
CC7.5	CM-01, CP-01, CP-04, CP-05, CP-06, IR-03, IR-04 Criteria also addressed via subservice provider controls.	The entity identifies, develops, and implements activities to recover from identified security incidents.
CC 8.0 Common Criteria Related to Change Management		
CC8.1	CM-02, CM-04, CM-05a, CM-05b, CM-06a, CM-06b, CM-07, CM-09, IR-03, SA-01, SA-03, SC-06, SI-08 Criteria also addressed via subservice provider controls.	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.
CC 9.0 Common Criteria Related to Risk Mitigation		
CC9.1	CP-01, CP-04, CP-05, CP-06, CP-07, CP-09, CP-12, CP-13, IR-03, IR-04 Criteria also addressed via subservice provider controls.	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.

Criteria	Controls List	Criteria
CC9.2	Criteria addressed via subservice provider controls.	The entity assesses and manages risks associated with vendors and business partners.
Additional Criteria for Availability		
A1.1	CM-01, CP-07, SC-03, SC-08 Criteria also addressed via subservice provider controls.	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.
A1.2	CP-01, CP-05, CP-06, CP-09, CP-12, CP-13, SC-03 Criteria also addressed via subservice provider controls.	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.
A1.3	CP-05, CP-06 Criteria also addressed via subservice provider controls.	The entity tests recovery plan procedures supporting system recovery to meet its objectives.
Additional Criteria for Confidentiality		
C1.1	CP-12 Criteria also addressed via subservice provider controls.	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.
C1.2	SI-09a, SI-09b	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.

Section V: Other Information Provided by Salesforce, Inc.

Management Responses to Exceptions Identified

Control Description	Exception Noted by EY	Management Response
AC-40: A quarterly analysis is performed to detect Termination and Transfers events not successfully triggered in the Identity Lifecycle Management tools. Identified events are investigated and resolved in accordance to the expected service-level agreement.	While the review was performed, the sampled review was performed 19 days after the required timeline.	Salesforce management is committed to continuously provide training and awareness for the control performers, to enhance the operation and execution of the control. As of November 15, 2022, Salesforce has implemented an automated procedure that will assist with the operational performance of the reviews.

Glossary of Terms

Listed below are commonly used terms throughout the Salesforce SOC reports. Any other terms will be defined in the report.

ACL	Access Control Lists
AICPA	American Institute of Certified Public Accountants
AWS	Amazon Web Services
BCP	Business Continuity Program
BIA	Business Impact Analysis
BOD	Board of Directors
CMT	Crisis Management Team
Company	Salesforce
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CSOCs	Complementary Subservice Organization Controls
CSF	Cybersecurity Framework
CSIRT	Computer Security Incident Response Team
DPA	Data Processing Addendum
FedRAMP	Federal Risk and Authorization Management Program
GRC	Governance, Risk and Compliance
IDS	Intrusion Detection System
IPE	Information Provided by the Entity
ISMS	Information Security Management System
ISO	International Organization for Standards
LLP	Limited Liability Partnership
MSA	Main Services Agreement
MFA	Multi-factor Authentication
NIST	National Institute of Standards and Technology
PCI-DSS	Payment Card Industry Data Security Standard
SLA	Service Level Agreement
SOC	System and Organization Controls
SPARC	Security, Privacy, and Architecture documentation
SR	Site Reliability
SSDL	Salesforce Secure Development Lifecycle
TLS	Transport Layer Security
U.S.	United States
VAP	Vendor Audit Program
V2MOM	Vision, Values, Methods, Obstacles and Measures