

System and Organization Controls (SOC2) Type 2

Salesforce Services on Hyperforce

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

For the Period February 1, 2023 to May 31, 2023

The Salesforce logo, which consists of the word "salesforce" in a white, lowercase, sans-serif font, centered within a blue, multi-lobed cloud-like shape.

salesforce



Table of Contents

Section I: Salesforce, Inc.'s Management Assertion	1
Section II: Independent Service Auditor's Assurance Report.....	3
Section III: Report on Management's Description of Salesforce, Inc.'s Salesforce Services on Hyperforce Covered Services System on the Suitability of the Design and Operating Effectiveness of Controls Relevant to Security, Availability, and Confidentiality for the Period February 1, 2023 to May 31, 2023	8
Overview of Operations	9
Salesforce Corporate Services and Salesforce Services Controls.....	9
Principal Service Commitments and System Requirements.....	10
Description of Covered Services.....	12
Overview of Salesforce Services on Hyperforce Covered Services Architecture	25
Services Provided by Subservice Organizations Excluded From the Scope of the Examination	26
Locations and Infrastructure	26
Software	27
People	27
Procedures	29
Customer Data.....	29
System Incident Disclosures.....	30
Relevant Changes	30
Relevant Aspects of the Control Environment, Risk Management, Monitoring, and Information and Communication	30
Control Environment.....	31
Risk Management.....	31
Monitoring.....	32
Information and Communication	32
Control Activities.....	32
General Information Systems Controls	32
Physical Security	32
Third Party Risk Management	32
Logical Security	32
Network Architecture and Management.....	36
Product Security	37
Threat and Vulnerability Management	37



Encryption	38
Change Management	38
Service Monitoring	40
Security Monitoring	40
Incident Management	41
Backup, Recovery, and System Availability	41
Contingency Planning and Business Continuity	42
Customer Data Deletion	42
Customer Control Responsibilities and Considerations	42
Complementary Subservice Organization Controls	43
Controls expected to be implemented at Salesforce Corporate Services.....	44
Controls expected to be implemented at other Salesforce Services on Hyperforce Subservice Organizations.....	47
Trust Services Criteria and Related Controls.....	49
Section IV: Salesforce, Inc.'s Criteria, Related Controls, and EY's Test Procedures and Results	50
Security, Availability, and Confidentiality Criteria, Related Controls, and EY's Test Procedures and Results	51
Purpose and Context.....	51
Trust Criteria and Related Controls for Systems and Applications	51
Procedures Performed for Assessing the Completeness and Accuracy of Information Provided by the Entity	52
Controls, Criteria, Tests, and Results of Tests	53
Criteria to Controls Mapping	69
CC 1.0 Common Criteria Related to Control Environment	69
CC 2.0 Common Criteria Related to Communication and Information	69
CC 3.0 Common Criteria Related to Risk Assessment	69
CC 4.0 Common Criteria Related to Monitoring Activities	70
CC 5.0 Common Criteria Related to Control Activities	70
CC 6.0 Common Criteria Related to Logical and Physical Access Controls.....	71
CC 7.0 Common Criteria Related to System Operations	72
CC 8.0 Common Criteria Related to Change Management	72
CC 9.0 Common Criteria Related to Risk Mitigation	73
Additional Criteria for Availability.....	73
Additional Criteria for Confidentiality	73

Section I: Salesforce, Inc.'s Management Assertion

The Salesforce logo, which consists of the word "salesforce" in a white, lowercase, sans-serif font, centered within a blue, multi-lobed cloud-like shape.

salesforce



Salesforce, Inc.'s Management Assertion

We have prepared the accompanying Report on Management's Description of Salesforce, Inc.'s Salesforce Services on Hyperforce Covered Services System on the Suitability of the Design and Operating Effectiveness of Controls Relevant to Security, Availability, and Confidentiality For the Period February 1, 2023 to May 31, 2023 (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 on Hyperforce Covered Services system (System) that may be useful when assessing the risks arising from interactions with the System throughout the period February 1, 2023 to May 31, 2023, 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 on Hyperforce 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 on Hyperforce 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 February 1, 2023 to May 31, 2023 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 February 1, 2023 to May 31, 2023.
- c. The Salesforce, Inc. controls stated in the Description operated effectively throughout the period February 1, 2023 to May 31, 2023 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 February 1, 2023 to May 31, 2023.

Salesforce, Inc.

Section II: Independent Service Auditor's Assurance Report

The Salesforce logo, which consists of the word "salesforce" in a white, lowercase, sans-serif font, centered within a blue, multi-lobed cloud-like shape.

salesforce

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 on Hyperforce Covered Services System on the Suitability of the Design and Operating Effectiveness of Controls Relevant to Security, Availability, and Confidentiality For the Period February 1, 2023 to May 31, 2023 (Description) of its Salesforce Services on Hyperforce 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 February 1, 2023 to May 31, 2023 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 on Hyperforce Covered Services system uses Salesforce Corporate Services Covered Services and Salesforce 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 on Hyperforce 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 on Hyperforce Covered Services' service commitments and system requirements based on the applicable trust services criteria. 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 February 1, 2023 to May 31, 2023.

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) selecting the trust service criteria applicable to the Description; (2) preparing the Description and Assertion; (3) the completeness, accuracy, and method of presentation of the Description and Assertion; (4) providing the services covered by the Description; (5) identifying the risks that would threaten the achievement of the service organization’s service commitments and system requirements; and (6) 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*, issued 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 on Hyperforce Covered Services system that was designed and implemented throughout the period February 1, 2023 to May 31, 2023 in accordance with the Description Criteria.

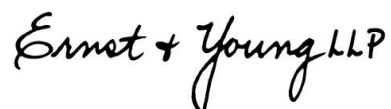
- b. the controls stated in the Description were suitably designed to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria if the controls operated effectively and if the Component and Non-affiliated Subservice Organizations (collectively, Subservice Organizations) applied the controls assumed in the design of Salesforce, Inc.'s controls throughout the period February 1, 2023 to May 31, 2023.
- 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 February 1, 2023 to May 31, 2023, if the Subservice Organization controls assumed in the design of Salesforce, Inc.'s controls operated effectively throughout the period February 1, 2023 to May 31, 2023.

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 on Hyperforce Covered Services system during some or all of the period February 1, 2023 to May 31, 2023, 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.



July 19, 2023

Section III: Report on Management's
Description of Salesforce, Inc.'s Salesforce
Services on Hyperforce Covered Services
System on the Suitability of the Design and
Operating Effectiveness of Controls
Relevant to Security, Availability, and
Confidentiality For the Period
February 1, 2023 to May 31, 2023

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 on Hyperforce Covered Services system or Covered Services).

Hyperforce is a public cloud optimized architecture developed by Salesforce that provides a set of foundational services and design patterns utilized by various Salesforce products and services. These foundational services provide a consistent and shared approach within public cloud architecture while providing a unified architecture baseline for service teams to deploy and manage their service(s).

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 and Salesforce Services Controls

This report should be reviewed in conjunction with the Salesforce Corporate Services and Salesforce Services SOC reports for details regarding the domains where the Salesforce Services on Hyperforce Covered Services system relies on corporate controls and Salesforce Services controls. 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

- Third Party Risk Management (TPRM)
- 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

Salesforce Services teams are responsible for all or a portion of the following domains:

- Change Management
- Encryption
- Database Engineering
- Application Protection
- Data Deletion

The above domains are covered as part of the Salesforce Corporate Services and Salesforce Services SOC reports.

Principal Service Commitments and System Requirements

Salesforce leverages advanced technologies along with the administrative, technical, and physical controls to help ensure the security, availability, and confidentiality of the Salesforce Services on Hyperforce Covered Services system. Salesforce's Trust and Compliance commitments to customers are communicated via MSAs, 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
 - Salesforce is committed to mitigate the risk of single points of failures and provide a resilient environment to support service availability, continuity, and performance.
- Architecture and data segregation
 - Salesforce products and services are operated in multitenant architecture that is designed to segregate and restrict customer access to data.

- Security controls
 - Salesforce security controls are designed and monitored continuously to protect the Company from threats and customer data from risk of unauthorized disclosure.
- Security policies and standards
 - Salesforce policies and standards are designed, implemented, and monitored to protect the Company from threats and customer data from risk of unauthorized disclosure.
- Security logging
 - Security logs are centralized, monitored and retained according to applicable data retention laws.
- Incident management
 - Salesforce notifies impacted customers of any unauthorized disclosure of their respective customer data by Salesforce or its agents of which Salesforce becomes aware to the extent permitted by law.
- User authentication
 - Salesforce implements industry leading practices to secure authentication to all Salesforce products and services.
- Physical security
 - Salesforce production data centers and public cloud providers used to provide Salesforce products and services have access control systems that permit and restrict only authorized personnel to have access to secure areas.
- Reliability and backup
 - All components of Salesforce products and services are configured in a redundant manner with backup policies and defined metrics.
- Disaster recovery
 - Salesforce disaster recovery plans are tested at least annually and are updated if necessary.
- Data encryption
 - Salesforce is committed to protecting customer data via deployment and use of applicable data encryption technologies
- Deletion of Customer Data
 - Salesforce is committed to securely overwrite or delete customer data from production in a timely manner upon customer request or contract termination.



The Salesforce Services on Hyperforce SPARC documents are managed and updated by the Legal organization, with input and collaboration from relevant stakeholders. The Salesforce Services on Hyperforce SPARC documents are reviewed and updated at least annually and as needed. The Trust and Compliance commitments for the Salesforce Services on Hyperforce Covered Services system that form the basis for the description of the controls herein are defined in the Salesforce Services on Hyperforce SPARC document published May 5, 2023.

Description of Covered Services

Salesforce Services on Hyperforce is responsible for components of infrastructure (i.e., software that comprise the Salesforce Services on Hyperforce 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 on Hyperforce Covered Services system described below:

Service Name	Service Description
Sales Cloud	<p>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.</p> <p>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.</p>

Service Name	Service Description
Service Cloud	<p>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.</p> <p>Salesforce Surveys</p> <p>Salesforce Surveys is a survey tool built natively on the Salesforce Platform. Customers can collaborate to create 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.</p> <p>Einstein Next Best Action</p> <p>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.</p>
Salesforce Mobile App (iOS/Android)	<p>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.</p>
Experience Cloud (formerly branded as Community Cloud)	<p>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 easily between them. Multiple communities can be created within the user organization for different purposes.</p>
Chatter	<p>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.</p>

Service Name	Service Description
Lightning Platform (including Force.com and Salesforce Connect)	<p>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 point-and-click customization tools to help customers without any programming experience create their own solutions for their business requirements.</p> <p>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 is stored outside of the customer's org.</p>
Site.com	<p>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.</p>
Database.com	<p>The Database.com platform is a stripped-down Salesforce Platform that provides a low-cost option for development in the cloud. It has a 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.</p>

Service Name	Service Description
CRM Analytics (formerly branded as Tableau CRM (including Einstein Discovery, Salesforce Data Pipelines and Headless Browser Service))	<p>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.</p> <p>Einstein Discovery</p> <p>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.</p> <p>Salesforce Data Pipelines</p> <p>Salesforce Data Pipelines provide fast and scalable data processing that extract, transform, and load (ETL) for the customer Salesforce org, supporting external data and machine learning powered data transformation.</p> <p>Headless Browser Service</p> <p>CRM Analytics' Headless Browser Service is a fast and scalable service that runs Analytics assets (Reports, Dashboards and CRM Analytics Dashboards), as a specific user, in a headless browser and generates realtime images. The service returns an encoded string to Salesforce, which can be converted into an image and used in Salesforce or Slack applications.</p>
IoT Explorer (including IoT Plus)	<p>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.</p>

Service Name	Service Description
Salesforce Shield	<p>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.</p> <p>Salesforce Platform Encryption</p> <p>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.</p> <p>Salesforce Event Monitoring</p> <p>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.</p> <p>Salesforce Field Audit Trail</p> <p>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.</p>
WDC	<p>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, real-time coaching, and full-featured performance reviews.</p> <p>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.</p>

Service Name	Service Description
Industry Clouds	<p>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:</p> <p>Health Cloud</p> <p>Health Cloud is designed to support the healthcare and life sciences (HLS) industries, including healthcare providers, payers, 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.</p> <p>Financial Services Cloud</p> <p>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.</p> <p>Manufacturing Cloud</p> <p>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.</p>

Service Name	Service Description
Industry Clouds (continued)	<p>Public Sector Solutions</p> <p>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.</p>
<p>Salesforce Configure Price Quote (CPQ) and Salesforce Billing (together formerly branded as Quote to Cash (QTC))</p>	<p>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.</p> <p>Salesforce Configure Price Quote (CPQ)</p> <p>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.</p> <p>Salesforce Billing</p> <p>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.</p>
<p>B2B Commerce (formerly branded as CloudCraze) and B2B Commerce on Lightning Experience</p>	<p>Salesforce B2B Commerce (B2BC) 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.</p>
<p>Salesforce Private Connect</p>	<p>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.</p>

Service Name	Service Description
Salesforce.org	<p>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:</p> <p>Nonprofit Success Pack (NPSP)</p> <p>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:</p> <ul style="list-style-type: none"> • Constituent and Donor Management • Donation and Grant Management • Engagement Management • Volunteer Management • Reporting and Analytics • Mobile, Social, and Cloud <p>Program Management Module (PMM)</p> <p>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.</p> <p>Nonprofit Cloud Case Management</p> <p>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:</p> <ul style="list-style-type: none"> • 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)	<p>foundationConnect</p> <p>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.</p> <p>Grants Management</p> <p>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 funding processes and more time driving their philanthropic mission.</p> <p>Education Data Architecture (EDA)</p> <p>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.</p> <p>Student Success Hub (formerly branded as Salesforce Advisor Link)</p> <p>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.</p> <p>Admission Connect</p> <p>Built on EDA (Education Data Architecture), Admissions Connect is a recruiting and admissions tool that streamlines application review, drives applicant engagement and facilitates collaboration across teams. Admissions Connect helps teams meaningfully engage applicants and effectively manage admissions processes.</p>

Service Name	Service Description
Workplace Command Center	<p>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.</p> <p>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.</p>
Platform Events (including Change Data Capture)	<p>Platform Events enables developers to deliver secure, scalable, and customizable event notifications within the Salesforce platform or from external sources.</p> <p>Customers use Platform Events to connect business processes in Salesforce and external apps through the exchange of real-time event data.</p> <p>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.</p> <p>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.</p>
Salesforce Identity	<p>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.</p>

Service Name	Service Description
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 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 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, customers have access to tools that facilitate collaboration, project management, and reporting.
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 users to plan and design loyalty programs, manage members, and partners. Customers can also track members' activities, reward members, drive engagement, and launch innovative promotions and offers.
Salesforce Slack Integration Proxy	The Salesforce Slack Integration Proxy provides a way to build Slack apps that run app logic in Salesforce. In order for requests and data to flow between Slack and Salesforce, a proxy is used for routing requests to the right org where the logic lives and will be executed.

Service Name	Service Description
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.
Enhanced Messaging	Agents respond to incoming messages directly from the service console. Customers can start conversations with your company over a channel of their choice, including Enhanced Messaging
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, and Document Generation)	<p>Decision Tables</p> <p>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.</p> <p>Data Processing Engine</p> <p>Data Processing Engine helps customers transform data that is 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.</p> <p>OmniStudio</p> <p>OmniStudio provides a suite of services, components, and data model objects that combine to create Industry Cloud applications. Create guided interactions using data from Salesforce org and external sources. With OmniStudio, customers may be enabled to create:</p> <ul style="list-style-type: none"> • 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. <p>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.</p> <p>Document Generation</p> <p>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.</p> <p>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.</p>
Unified Messaging	<p>Unified Messaging enables brands to communicate with their customers securely and at scale via Email, SMS, and WhatsApp engagement channels. It honors recipient consent from Privacy Center at send time, renders personalized, branded content based on Data Cloud data, and enriches Data Cloud profiles by tracking deliverability disposition and engagement per recipient.</p>

Service Name	Service Description
Salesforce Contracts	<p>Salesforce Contracts is a contract lifecycle management tool that enables businesses to efficiently and collaboratively manage their contracting process, right from authoring and negotiations through approval, execution, renewal and amendments. Salesforce Contracts provides a highly usable, configurable, and extensible platform that delivers contracting processes for industry-specific use cases.</p> <p>Note: This report addresses Salesforce Contracts components built on Salesforce Services. The OmniStudio managed package that Salesforce Contracts leverages is covered in the Vlocity SOC Reports.</p>
Nonprofit Cloud	<p>Nonprofit Cloud helps unite teams with a purpose built system for funding, delivering and measuring impact. It includes features and products developed using the power of the Salesforce platform. Taking advantage of this technology, provides faster, easier access to Salesforce's full portfolio of innovative products and services.</p>
Automotive Cloud	<p>Automotive Cloud is Salesforce's industry-specific platform for the automotive industry. Automotive Cloud brings OEMs, Retails, and Finance Groups together around a unified view of vehicle, customer, and retail data to drive loyalty, customer lifetime value, and revenue. With Automotive Cloud, automakers along with the extended automotive ecosystem can work collaboratively to better respond to market needs, drive retail sales, and improve customer satisfaction.</p>

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

Overview of Salesforce Services on Hyperforce 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.

Hyperforce provides the foundational infrastructure for Salesforce product and service teams to deploy applications into the public cloud. The foundational services provide configured public cloud resources allocated to products and services, referred to as functional domains. Each functional domain comes with its own isolated private network. Within a functional domain, compute workloads such as virtual machines (VMs) and containers can directly address each other over this private network. In contrast, communication across functional domains is done via load balancers, message queues, and/or API gateways. Communication over both public and private networks is encrypted using Transport Layer Security (TLS) or similar, and requires connections to be authenticated/authorized.



Hyperforce relies on automated version control of deployed operating systems and application services to prohibit any unauthorized changes from being deployed. Changes are made by building new compute workloads and replacing the existing instances.

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 provided by AWS
Salesforce Services	Controls and processes provided by Salesforce Services' Covered Services

Locations and Infrastructure

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

Function	Description
Operations Support	Operations support is in the following locations: <ul style="list-style-type: none">• San Francisco, California (Headquarters)• Northern Virginia, USA• Bellevue, Washington• Hyderabad, India• Dublin, Ireland• Singapore, Singapore• Sydney, Australia
Public Cloud Service Providers	The Covered Services has infrastructure hosted on AWS in data centers. Salesforce, Inc. maintains a current list of AWS locations supporting the Covered Services on its public webpage .

More information regarding the specific infrastructure, locations, and controls is contained within the Salesforce Services on Hyperforce Trust and Compliance documentation on <https://trust.salesforce.com/>. For further details on this section with regards to controls supported by Corporate Services and Salesforce Services, please refer to the Salesforce Corporate Services and Salesforce 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.
Data Stores	Persistent Customer Data resides in databases and cloud object storage instances.
Monitoring Systems	There are multiple monitoring systems in use for the Covered Services, including: <ul style="list-style-type: none"> • Security incident event monitoring • Performance monitoring system
Network Infrastructure	The Covered Services network infrastructure utilizes a common set of network components, including: <ul style="list-style-type: none"> • Security Groups • Cloud Domain Name Systems (DNS) Web Service

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

Corporate Services Team	Responsibilities Covered
Security	Salesforce Services on Hyperforce inherits security responsibilities from Salesforce Corporate Services. For further details regarding this section, please refer to the Salesforce Corporate Services SOC report.

Hyperforce Team	Responsibilities Covered
Infrastructure Engineering	<p>For Systems:</p> <ul style="list-style-type: none"> • Service configuration & management • Setup access to servers • Disaster recovery <p>For Network:</p> <ul style="list-style-type: none"> • Network device configuration & management • Setup access to network • Define network security standards • Implement and review security groups • Capacity planning
Development/Quality Engineering	<ul style="list-style-type: none"> • Develop new code, fix bugs • Release management • Write technical specifications and performance software build services
Program/Product Management	<ul style="list-style-type: none"> • Provide development project/product management, release/deployment management and status reporting • Identify customer requests and prioritize functionality to be released
Site Reliability (SR) Engineering	<ul style="list-style-type: none"> • Provide performance incident management for critical incidents within the Salesforce environment

Salesforce Services on Hyperforce Team	Responsibilities Covered
Database Engineering	<ul style="list-style-type: none"> • Database configuration & management, including backup and retention • Setup access to database instances • Data protection
Development/Quality Engineering	<ul style="list-style-type: none"> • Develop new code, fix bugs • Release management • Write technical specifications and performance software build services
Program/Product Management	<ul style="list-style-type: none"> • Provide development project/product management, release/deployment management and status reporting • Identify customer requests and prioritize functionality to be released

For further details on this section with regards to controls supported by Salesforce Corporate Services and Salesforce Services, please refer to the Salesforce Corporate Services and Salesforce 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. Extractions are documented, tracked, and encrypted, which is 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	<p>Inclusion of Unified Messaging, Salesforce Contracts, Nonprofit Cloud, and Automotive Cloud in the scope of the Salesforce Services on Hyperforce Covered Services.</p> <p>Removal of Salesforce Hub from the scope of the Salesforce Services on Hyperforce Covered Services as the service has been deprecated.</p>
Control Change	<p>Removal of Control 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.</p> <p>Due to the enhanced security mechanisms associated with the employment of Just-in-Time (JIT) access required for the Hyperforce production environment, a manual lookback analysis was deemed no longer necessary as a key control for the Covered Services to meet the trust services criteria.</p>

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 service commitments and system requirements.

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 Governance, Risk, and Compliance (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 help 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. Further details of physical security at Salesforce Corporate Offices 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.

Third Party Risk Management

The Salesforce Security GRC team includes a Third Party Risk Management (TPRM) Program 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

Access to the Salesforce Services on Hyperforce Covered Services production environment is role-based and restricted to authorized personnel utilizing the principle of least privilege. Users are required to adhere to a set of predefined requirements prior to requesting production access via the self-service identity management portal. These requirements include a completed background investigation, completion of change management training, 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. After the request is approved by their manager, a production user account is automatically provisioned by the identity lifecycle management tool. There are two types of production access: Application Access (including access to AWS Console) and Host Access.

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 enforce 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.

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 to use one of the predefined Salesforce Security approved IAM roles applied to the environment upon creation. 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. Read-only access to the console cannot exceed 31 days in duration, and any level of privileged access above read-only cannot exceed seven days in duration.

Read-only access to production hosts is persistent for users who have met the aforementioned prerequisites. Access is role-based and limited only to production hosts approved by the user's manager upon the provisioning of the production user account. Elevated access, including sudo and any access above read-only, is separately managed through a JIT dashboard which requires an elevation request and approval. Each elevation request is only valid for a defined period and elevated access can be revoked if needed.

Customer access to the Salesforce Services on Hyperforce Covered Services application is the responsibility of the customer. New customers sign/acknowledge an MSA, which includes considerations for protecting the security, confidentiality, and integrity of data. Customers are provided access to their environment by a designated Salesforce system administrator 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. For further details regarding this section, please refer to the Salesforce Corporate Services SOC report.

Access to databases hosted on Salesforce Services on Hyperforce is achieved through sudo/elevated permissions and JIT access requests. Before new databases are brought into the production environment, default database vendor accounts are locked and passwords are changed or removed to prevent unauthorized access.

Service accounts are deployed and utilized to manage service integrations within the Covered Services production environment. A secure vault restricted to authorized personnel is used to protect the service account passwords. Passwords for service accounts utilized to manage service integrations are rotated at least every 90 days.

Access Authentication

Prior to authentication to Salesforce Services on Hyperforce Covered Services production systems, individuals must be authenticated on Salesforce's Corporate Network utilizing valid Active Directory credentials. For further details regarding this section, please refer to the Salesforce Corporate Services SOC report.

Access to production systems is achieved with password-based authentication, enforced via multi-factor authentication (MFA), and dynamic password generation or password parameters set in accordance with company standards.

Public cloud management console access is managed via a JIT dashboard. The user is restricted to a defined period of time in which the user can access the production environment, which is automatically revoked when it reaches expiry. Additionally, users can only access the 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 MFA using their corporate network username, password and one-time passcode token.
- The second layer of authentication includes authentication to the public cloud console JIT dashboard which requires a production account username, password, and one-time passcode 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.

Read-only host access is persistent once a user has met the required prerequisites defined in the Account Provisioning section above. To access a production host and obtain elevated access, a user must pass through multiple layers of authentication described below:

- The first layer of authentication is through a secure virtual gateway and requires MFA using their corporate network username, password, and one-time passcode token.
- The second layer of authentication includes authentication to Production Remote Access (PRA) and the bastion host using a production account username and password. This requires a user to have been granted a production account as part of account provisioning and be assigned to a specific role enabling this level of access.
- The third layer is authentication to the individual production hosts where authorized users can login using single sign-on (SSO).

- The fourth layer is elevated access (sudo) authentication within the individual production hosts which requires the user to request elevation via a JIT dashboard. A user must be assigned a specific role to possess the ability to obtain privileged access at the host level.

Access Reviews

On a quarterly basis, management performs an access review of the users with the ability to grant JIT access, and the related administrators group, in the Salesforce Services on Hyperforce Covered Services production environment through the public cloud management console and grant JIT elevation (sudo) access at the host level. These are tracked within an internal ticketing system and verifies that terminated users have been removed from the respective systems and the access rights remain appropriate based on job functions. Deviations and necessary changes identified during the review are recorded and remediated. In the event terminated users with the ability to grant JIT access or members of the related administrators group are present at the time of the review, a lookback analysis is performed to help ensure these users did not improperly use those privileges.

Additionally, on an ongoing basis employee transfers are reviewed to determine that access to the production system is still appropriate. The review is initiated automatically following a change in the HR system to an employee's manager combined with additional change in an employee's job profile, company, cost center or business unit. The change triggers the automatic creation of a transfer review ticket, which has a defined workflow that requires the user's manager to review the transferred user's access for appropriateness. The manager has 30 days to complete the transfer review and close the ticket and access not reviewed within 30 days is revoked. If a change in user access is necessary a child ticket is created for each access to track the removal. Automated workflows are in place to enforce the access removals in alignment with Salesforce Security Standards. The automated workflows aforementioned do not extend to the users with the ability to grant JIT access through the public cloud management console and grant JIT elevation (sudo) access at the host level.

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.

For further details regarding this section, please refer to the Salesforce 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 two logically and physically separated networks: a corporate 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 regarding this section, please refer to the Salesforce Corporate Services SOC report.

In addition, non-production environments which support software development, quality assurance, and part of release engineering are logically segregated from the production environment.

Networking protocols that are unnecessary for business purposes and/or are deemed to be non-secure are disabled. Network access control lists (ACLs), security groups, and subnets are used to restrict inbound network access and information flow between the different networks.

Network traffic is monitored and logged. A predefined group of policies have been configured to generate an automatic notification to designated personnel when violations occur and, depending on the severity of the policy violation, appropriate levels of escalation are applied. For further details regarding the monitoring and resolution of identified violations, please refer to the Salesforce Corporate Services SOC report.

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.

Network Malware Detection

Malware and virus detection is in place on the corporate network, and alerts are generated in the event of compromise or potential compromise. For further details regarding this section, please refer to the Salesforce Corporate Services SOC report.

Application Protection

Customers connect to the Covered Services over the Internet 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.



An Internal Admin Portal is 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 application through special accounts to support customers. Support personnel 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. For further details on Salesforce's Internal Admin Portal and customer support controls, please refer to the Salesforce Services SOC report.

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 within the Salesforce Services on Hyperforce Covered Services production environment. 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. For further details regarding the monitoring and resolution of identified events, 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.

Payment Card Industry Data Security Standard 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. In addition, server side certificates for the Covered Services are rotated in accordance with the Cryptographic Key Management Standard.

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, standard fields, Chatter, files, attachments, and emails. Salesforce also offers a free encryption feature, Classic Encryption, available for custom fields that customers create. For further details of Salesforce's Platform Encryption offering, please refer to the Salesforce Services SOC report.

Customer Data at-rest stored in Salesforce Services on Hyperforce's Covered Services is encrypted, regardless of storage solution and stored in Amazon Elastic Block Storage (EBS) volumes attached to an Amazon Elastic Cloud Compute (EC2) instance and S3 blob storage buckets. The Hyperforce Infrastructure Engineering team has created configuration templates for services to utilize in order to securely configure their AWS resources to encrypt Customer Data at-rest, which includes configuring the Salesforce managed Customer Managed Key (CMK) for annual rotations. EBS volumes are automatically encrypted by default at the account level. Policies are in place to help ensure encryption is enabled and will block any resources from being created or modified if encryption requirements are not met. At-rest encryption of EBS volumes and S3 buckets is enabled with the Salesforce Managed key. The Hyperforce Infrastructure Engineering team utilizes Salesforce managed-CMKs to encrypt each EBS volume and S3 bucket. Encryption keys are fully managed by AWS and are not visible to customers. As part of its management, AWS handles rotation of CMKs via AWS Key Management Service (KMS), as configured by the Hyperforce Infrastructure Engineering team.

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.

To manage the change process, a change control system is used as the ticketing and tracking tool for the changes. The Covered Services uses industry recognized code versioning software for source control management and making changes to its repositories via pull requests. The change control system requires multiple criteria to be completed before a change can be pushed to production, including a link to the pull request, automated or manual tests, and approvals as defined for given change types. Testing includes two areas: change readiness testing and post-deployment verification testing. Change readiness testing determines whether a change case meets the expected requirements and can include unit, functional, scenario, stress, performance, and/or security testing. Post-deployment verification testing verifies that the change is successful through automated deployment testing. A change request is considered complete when the required fields are filled, and approvals are met.

Infrastructure Change Management

The change management process is a defined process that requires people, process, and technology to support the process. Changes to infrastructure components in public cloud environments are made through code utilizing industry standard Infrastructure as Code (IaC) software. Individuals who wish to deploy an IaC change into production are required to follow the defined Global Change Management Procedure and Change Management Security Standard, and to complete mandatory change management training before participating in the change management process. The Global Change Management Procedure defines the required approvals that a change must route through before the change owner 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 Procedure.

Infrastructure change management encompasses operational changes for maintaining the service at the network and database level. The majority of changes that are processed via the Salesforce infrastructure change process are Standard or Standard Pre-Approved changes. These changes are considered lower risk, routine operating activities and either follow an established pre-approved template or require a peer review approval; and are systematically implemented based on an 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, which has been pre-approved via the Change Advisory Board (CAB). These are limited to low-risk changes and typically include patching or other operational activities and have a consistent history of success and execution without errors. Standard changes are low-risk, performed frequently, use a defined template or run list, and require peer approval. 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. A pipeline will not deploy without an approved scheduled change case or a Standard Pre-Approved change template, which allows the pipeline to generate a case.

Application Change Management

Application change requests are documented and tracked through the online ticket management system and code repository. Desired application functionality and features are identified, prioritized, and initiated by product owners for future development. Information security, availability, and confidentiality

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 automated and/or manual testing prior to merging the changes into the master code that makes up a release. Application code releases with customer facing features and functionality changes are packaged into Salesforce Services releases. For further details regarding release processes, please refer to the Salesforce Services SOC report.

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. Production code changes must have approval prior to implementation into production.

The change management tools (code versioning software and online ticketing system) maintain a record of all 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.

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.

System capacity planning is conducted to help ensure necessary resources, including compute and data storage resources, are added as needed. The Capacity Planning team meets with the public cloud service provider on a weekly basis to discuss upcoming capacity orders, forecasts, and any issues. Each order is discussed to determine if capacity will be delivered on time and without issue. The public cloud service provider is then provided with a rolling forecast of the capacity required for upcoming builds.

The Salesforce Trust site is available for internal and external users. It contains information regarding service disruptions, system availability, and informational messages. In the event of an ongoing incident, Salesforce Services on Hyperforce Covered Services will provide ongoing reporting on the Salesforce Trust site as well.

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 on Hyperforce 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 Cyber Security Incident Response Team (CSIRT). For further details regarding this section, please refer to the Salesforce Corporate Services SOC report.

Availability Incident Management

The Salesforce Site Reliability Engineering team has built a variety of health indicators that serve to identify anomalous conditions in the health of the Salesforce Services on Hyperforce Covered Services. Many of these anomalies will be resolved via automated processes. Availability alerts that cannot be resolved using automated processes are handled by a rotating roster of on-call engineers. The on-call teams investigate performance and availability issues, create an incident channel, perform root cause analyses, develop and deploy fixes for the issues, and track the issues to completion in a ticketing system. Investigation and corrective actions for customer impacting performance incidents are documented and shared with key personnel to confirm corrective actions have been completed and lessons learned have been incorporated.

The Salesforce Trust site is available for internal and external users. It contains information around service disruptions, system availability, and informational messages. Further details of Salesforce's Trust site are found in the Salesforce Corporate Services SOC report.

Customer Incident Management

The Covered Services have onboarded to 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

The Hyperforce Contingency Plan establishes procedures to maintain business critical processes and meet availability and system requirements in the event of a declared business impacting disaster. Hyperforce data storage and processing is configured to be spread across multiple Availability Zones (AZs) in a region.

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 key personnel and recovery processes to be followed in the event of a declared disaster. A formal Disaster Recovery exercise is executed annually to test the effectiveness of the contingency planning and recoverability of Hyperforce services to meet recovery objectives. Results of the exercise are documented and made available internally. Lessons learned are incorporated into plan updates and are used to prepare resources for future exercises.

Salesforce Services on Hyperforce databases are replicated in real-time to protect Customer Data. Redundant instances are configured so primary databases are fully replicated to a secure, access controlled, and multi-zone secondary storage instance. Customer Data in application databases is backed up using at minimum quarterly full backups, daily incremental backups, and optional hourly archive log backups. Database backup success is monitored. Backup related issues, such as backup failures, are automatically reported to a dashboard.

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 are stored in S3 blob storage buckets are replicated across multiple availability zones (AZs). For further details on database backup and retention of customers' production data, please refer to the Salesforce Services SOC report.

Contingency Planning and Business Continuity

In addition to the Salesforce Services on Hyperforce 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 the subscriptions associated with an environment, Customer Data submitted to the Covered Services may remain in an inactive status within the Covered Services for up to 120 days, after which it is securely overwritten or deleted from production within 90 days, and from backups within 300 days. The data deletion process is monitored by a dashboard which enables tracking of Customer Org deletion in relation to data deletion timeline commitments. When Customer Orgs near or exceed predefined thresholds, alerts generate an automatic notification to designated personnel to investigate and take corrective action. For further details on Customer Data deletion, please refer to the Salesforce Services SOC report.

Customer Control Responsibilities and Considerations

This section describes additional customer control responsibilities and considerations. While these are not necessary for Salesforce Services on Hyperforce 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 MFA. 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.

Controls customer should consider implementing

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 accounts they have requested or created which may include: Salesforce Customer Support, Professional Services, or other Salesforce teams providing assistance with your 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.

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.

Complementary Subservice Organization Controls

Salesforce Services on Hyperforce 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 on Hyperforce utilizes Salesforce Services to provide customer support, application change management, and publishing of release notes to internal and external users via the Trust site. This report should be read in conjunction with the report issued by Salesforce, Inc. over the Salesforce Services' 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
<ul style="list-style-type: none"> 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
<ul style="list-style-type: none"> BOD independence and oversight over internal controls is established in the BOD charter and through regular communications to the BOD. 	CC1.2
<ul style="list-style-type: none"> 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
<ul style="list-style-type: none"> 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
<ul style="list-style-type: none"> 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
<ul style="list-style-type: none"> 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
<ul style="list-style-type: none"> 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
<ul style="list-style-type: none"> 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

Controls expected to be implemented at Salesforce Corporate Services	Complemented criteria
<ul style="list-style-type: none"> Trust sites are updated with advisories about security issues impacting customers. 	CC2.3, CC7.4, CC7.5
<ul style="list-style-type: none"> The Company has implemented security compliance audits, Business Continuity Program, Business Impact Analysis (BIA), Global Crisis Management Team Plan, incident response process, Third Party Risk Management, 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
<ul style="list-style-type: none"> The Company performs activities, such as compliance audits, to assess whether internal controls are present and functioning. 	CC4.1
<ul style="list-style-type: none"> Identified internal control deficiencies are managed, tracked, communicated and remediated as required. 	CC4.2
<ul style="list-style-type: none"> 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
<ul style="list-style-type: none"> Policies and standards that define control activities are documented, communicated, and reviewed periodically. 	CC5.3
<ul style="list-style-type: none"> 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
<ul style="list-style-type: none"> 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. 	CC6.1, CC6.7, CC8.1
<ul style="list-style-type: none"> 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

Controls expected to be implemented at Salesforce Corporate Services	Complemented criteria
<ul style="list-style-type: none"> 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 Third Party Risk Management (TPRM) prior to processing Customer Data. TPRM performs supplier due-diligence reviews for all Tier 1 suppliers on a calendar year basis to monitor compliance with Salesforce security requirements. Any issues identified are evaluated and remediated in a timely manner. 	CC6.4, CC6.5, A1.2
<ul style="list-style-type: none"> 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
<ul style="list-style-type: none"> The Company has implemented a threat and vulnerability management program to identify and respond to vulnerabilities. 	CC7.1, CC7.2
<ul style="list-style-type: none"> The Company has a centralized team to track and resolve security issues identified in the products and services. 	CC6.8, CC7.1
<ul style="list-style-type: none"> 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
<ul style="list-style-type: none"> The Company has a customer support function for escalating and resolving incoming customer cases. 	CC7.3, CC7.4
<ul style="list-style-type: none"> Cyber Security Incident Response Team (CSIRT) has defined processes to evaluate, escalate, track and resolve identified security incidents. 	CC7.3, CC7.4, CC7.5
<ul style="list-style-type: none"> The Company maintains a Change Management Standard which defines the requirements for performing changes, and is reviewed annually. 	CC8.1
<ul style="list-style-type: none"> 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 on Hyperforce Subservice Organizations

Controls expected to be implemented at Public Cloud Providers	Complemented criteria
<ul style="list-style-type: none"> 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
<ul style="list-style-type: none"> Additions and changes to the system are authorized prior to access being granted. System access is removed timely upon termination. 	CC6.2
<ul style="list-style-type: none"> 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
<ul style="list-style-type: none"> 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
<ul style="list-style-type: none"> Production media is securely decommissioned and physically destroyed prior to leaving the data center. 	CC6.5
<ul style="list-style-type: none"> External vulnerability assessments are performed on a periodic basis, identified issues are investigated and tracked to resolution in a timely manner. 	CC7.1
<ul style="list-style-type: none"> Changes are authorized, tested, and approved prior to implementation. 	CC8.1

Controls expected to be implemented at Public Cloud Providers	Complemented criteria
<ul style="list-style-type: none"> Production data in blob storage is replicated near real-time from the primary site to a secondary site. 	CC9.1, A1.2
<ul style="list-style-type: none"> Public cloud provider protects against or limits the effect of denial of service attacks. 	A1.1
<ul style="list-style-type: none"> Environmental protections have been installed including the following: <ul style="list-style-type: none"> Cooling systems Battery and generator backups Smoke detection Dry pipe sprinklers Environmental protection equipment receives maintenance on at least an annual basis. 	A1.2
<ul style="list-style-type: none"> Backups of critical system components are monitored for successful replication across multiple data centers. 	A1.3
Controls expected to be implemented at Salesforce Services	Complemented criteria
<ul style="list-style-type: none"> Customers are uniquely identified and authenticated and cannot access the environment without a valid user ID and password. 	CC6.1, CC6.2
<ul style="list-style-type: none"> 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
<ul style="list-style-type: none"> Activities performed by support personnel using the login as functionality for a given customer are logged and available for customer review. 	CC5.2
<ul style="list-style-type: none"> Application releases into production do not occur until appropriate sign-offs are obtained and documented. 	CC6.1, CC8.1
<ul style="list-style-type: none"> Release notes are documented and communicated to internal and external users for changes and maintenance that affect system security, availability and confidentiality. 	CC2.2, CC2.3
<ul style="list-style-type: none"> The Cryptographic Key Management Standard specifies the encryption key management and storage requirements, and is reviewed/updated on an annual basis. 	CC6.1
<ul style="list-style-type: none"> Internal Admin Portal user access is revoked in a timely manner upon termination. 	CC6.1, CC6.2, CC6.3

Controls expected to be implemented at Salesforce Services	Complemented criteria
<ul style="list-style-type: none"> Salesforce Services application logical access is reviewed by management on a quarterly basis. Accounts identified as not appropriate are investigated and resolved. 	CC6.2
<ul style="list-style-type: none"> Code versioning software is used during the systems development life cycle to support rollback. 	CC8.1
<ul style="list-style-type: none"> Application security controls prevent customers from accessing data of other customers. 	CC6.1
<ul style="list-style-type: none"> Salesforce Services is responsible for database configuration and management, including data protection. 	CC8.1, CC9.1
<ul style="list-style-type: none"> 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
<ul style="list-style-type: none"> Salesforce Services encrypts Customer Data based on the Customer's selection of platform encryption or field level encryption. 	CC6.1
<ul style="list-style-type: none"> Platform Encryption keys are rotated each major release in accordance with the Cryptographic Key Management Standard. 	CC6.1
<ul style="list-style-type: none"> Application changes are documented and tracked in an internal ticketing system. 	CC2.1, CC5.2, CC5.3, CC6.8, CC8.1
<ul style="list-style-type: none"> Application code changes are tested and/or peer reviewed prior to implementation into production. 	CC8.1
<ul style="list-style-type: none"> Salesforce Services disposes confidential Customer Data on databases and monitors the deletion process via a dashboard per commitments made to the customer. 	CC1.2

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 on Hyperforce Covered Services system as described in Section III.

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

The Salesforce logo, which consists of the word "salesforce" in a white, lowercase, sans-serif font, centered within a blue, multi-lobed cloud-like shape.

salesforce

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, Inc. 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	<p>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.</p> <p>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.</p> <p>Availability Criteria Information and systems are available for operation and use to meet the entity's service commitments and system requirements.</p> <p>Confidentiality Criteria Information designated as confidential is protected to meet the entity's service commitments and system requirements</p>
Controls	<p>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, Salesforce Services, and AWS, which are defined Section III, are required to achieve the applicable criterion for Security, Availability, and Confidentiality. The Salesforce Corporate Services, Salesforce Services, and AWS SOC reports should be read in conjunction with the Salesforce Services on Hyperforce Covered Services system report.</p>

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.	<u>CC6.1</u> , <u>CC6.2</u> , <u>CC6.3</u> , <u>CC7.1</u>	Inspected authentication policy documentation to determine requirements for appropriate identification and authentication credentials, including multi-factor authentication, were defined.	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.
		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.
AC-07: Secure encryption algorithms are used to remotely manage production infrastructure.	<u>CC6.7</u> , <u>CC6.8</u>	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.
		Inspected the production management console TLS certificate to determine TLS cryptographic protocols were used.	No exceptions noted.

Control Description	SOC 2 Criteria Reference	EY's Test Procedures	EY's Test Results
AC-13a: New access to the production environment is provisioned and enforced using automated mechanisms and to only individuals which have been specifically authorized and approved after the completion of defined prerequisites.	<u>CC6.1</u> , <u>CC6.2</u> , <u>CC6.3</u>	Inspected the Onboarding requirements to determine prerequisites prior to granting new access to production environment were defined along with access approval requirements.	No exceptions noted.
		Inspected system configurations within the access management console and ILM tool to determine it was configured to enforce completion of required pre-requisites and manager approval prior to access being granted.	No exceptions noted.
		Inspected the case history details for a sample new user to determine the required pre-requisites were completed and access was approved by management prior to being granted.	No exceptions noted.
		Observed a user attempt to request access without having completed the required prerequisites to determine the access request was not permitted.	No exceptions noted.
AC-13b: Pre-defined access roles and permissions are applied to public cloud environments upon creation and the ability to modify the permission boundary rules is restricted.	<u>CC6.1</u> , <u>CC6.2</u> , <u>CC6.3</u>	Inspected the Public Cloud Security Standard to determine security control requirements for cloud service providers were defined.	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.

Control Description	SOC 2 Criteria Reference	EY's Test Procedures	EY's Test Results
		Inspected system configurations within the code repository to determine permission boundary rules were enforced for all public cloud role creations to restrict any role, other than the AccountSetup Role from having the access to create new users and roles, and restrict 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 without the AccountSetup Role attempt to create a new customer user and role and determine the system prevented the actions.	No exceptions noted.
		Observed a user attempt to modify the boundary permissions for a role outside of PCSK to determine the system prevented the actions.	No exceptions noted.
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 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.	No exceptions noted.
		Inspected the termination record for a sample terminated user to determine the users' access to the target production system was systematically removed based on the termination date.	No exceptions noted.

Control Description	SOC 2 Criteria Reference	EY's Test Procedures	EY's Test Results
		Inspected details for a sample of automated termination failures, selected from the ticketing system, to determine the issues were resolved and the user's access was removed within 5 business days.	Per inspection of a query from the ticketing system, EY determined there were no termination failures within the examination period.
AC-17: Production user access is reviewed for role changes and transfers. Issues identified are investigated and resolved within 30 days of transfer.	<u>CC5.2</u> , <u>CC5.3</u> , <u>CC6.2</u> , <u>CC6.3</u>	Inspected system configuration to determine in the event of a transfer as noted in the HR system, ILM initiates a review of the access and any access not approved after a defined period of time or noted as rejected by the reviewer is systematically removed.	No exceptions noted.
		Inspected the transfer review record in ILM to determine the access was systematically removed when the access was not approved by the reviewer.	No exceptions noted.
AC-18: Administrative access to approve temporary user access to production infrastructure components and public cloud administration consoles is reviewed on a quarterly basis. Accounts identified as not being appropriate are investigated and resolved.	<u>CC6.2</u>	Inspected the Access Management policy to determine requirements and guidance to perform user access reviews were defined.	No exceptions noted.
		Inspected the access review ticket details and supporting evidence for a sample quarter for a sample of in-scope service components to determine a quarterly access review of administrative access who can approve temporary user access to production infrastructure components and public cloud administration consoles was performed, and any issues identified 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.	<u>CC6.2</u>	Inspected Access Management standard documentation 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-22a: Vendor provided database accounts are locked, removed or the default password is changed.	<u>CC6.2</u> , <u>CC6.6</u>	Inspected Salesforce's Vendor Hardening Guide to determine default vendor 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 system configurations within the code repository and the vendor / service account status for a sample database to determine vendor / service accounts were locked or removed, or the default password was changed.	No exceptions noted.
AC-22b: Passwords for service accounts utilized to manage service integrations are maintained in a secure password vault which is restricted to authorized personnel.	<u>CC6.2</u> , <u>CC6.6</u>	Inspected password vault configurations to determine passwords for the database service accounts used to manage service integrations were maintained securely, and access was restricted to authorized personnel.	No exceptions noted.
		Inspected the job title, reporting chain, and performed inquiry of the control owner for the list of users with access to the password vault to determine access was restricted to authorized personnel.	No exceptions noted.

Control Description	SOC 2 Criteria Reference	EY's Test Procedures	EY's Test Results
AC-22c: Passwords for service accounts utilized to manage service integrations are rotated every 90 days.	<u>CC6.2</u> , <u>CC6.6</u>	Inspected Salesforce's Authentication Standard to determine it documented the requirements on password rotation for service accounts.	No exceptions noted.
		Inspected the ticket details for a sample quarterly rotation to determine the passwords for services accounts utilized to manage service integrations were rotated on a periodic basis.	No exceptions noted.
AU-02a: Production cloud administration consoles, servers, and databases are configured to log privileged operations, authorized access, and unauthorized access attempts.	<u>CC2.1</u> , <u>CC5.2</u> , <u>CC7.2</u>	Inspected baseline configurations for production infrastructure within the configuration management system to determine production infrastructure was configured to log privileged operations, including authorized and unauthorized access attempts.	No exceptions noted.
		Observed an authentication attempt and inspected the corresponding details within the centralized logging system to determine the event was logged.	No exceptions noted.
AU-02b: Production cloud administration console, server and database logs are transmitted to a centralized logging system.	<u>CC2.1</u> , <u>CC5.2</u> , <u>CC7.2</u>	Inspected baseline configurations for production infrastructure within the configuration management system to determine production infrastructure was configured to transmit logs to a centralized logging system for monitoring.	No exceptions noted.
		Observed an authentication attempt 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.	<u>CC2.1</u> , <u>CC7.2</u>	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.

Control Description	SOC 2 Criteria Reference	EY's Test Procedures	EY's Test Results
		Inspected NTP configurations for a sample production host to determine production information processing systems were configured to synchronize with a centralized NTP server.	No exceptions noted.
AU-08: Infrastructure as code deployment pipelines are configured to check changes for security policy violations, and block changes which violate defined policies.	<u>CC2.1</u> , <u>CC5.2</u> , <u>CC7.2</u>	Inspected system configurations for a sample of policy agents selected from the code repository to determine policy agents were enabled for code deployment pipelines to check for and prevent implementation of code that resulted in defined security policy violations.	No exceptions noted.
		Inspected an attempt to execute an operation which violated the configured security policy and determined the operation was systematically blocked.	No exceptions noted.
		Inspected configurations for a sample of mandatory deny OPA policies selected from the code repository to determine the policy was configured to check changes for security policy violations and block problematic code.	No exceptions noted.
CM-01: Capacity planning is conducted and monitored so that necessary capacity for long term strategic planning exists.	<u>CC4.1</u> , <u>CC7.5</u> , <u>A1.1</u>	Inspected meeting invite details and capacity planning agenda for the recurring weekly Capacity Planning meetings to determine the periodic execution of strategic capacity planning.	No exceptions noted.
		Inspected monitoring dashboards to determine that capacity monitoring and capacity planning schedules for production systems were in place.	No exceptions noted.

Control Description	SOC 2 Criteria Reference	EY's Test Procedures	EY's Test Results
CM-02: A version management system is utilized to maintain current and prior configurations for public cloud environments, control plane systems, and infrastructure components.	<u>CC2.1</u> , <u>CC7.1</u> , <u>CC8.1</u>	Inspected the version management system to determine current and prior configurations for public cloud environments, control plane systems, and infrastructure components were maintained and could support roll-back if necessary.	No exceptions noted.
CM-05a: Production code deployments are documented, tested, and peer reviewed and/or approved by management.	<u>CC6.1</u> , <u>CC6.8</u> , <u>CC8.1</u>	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 system configurations within the code repository to determine changes were required to complete peer reviews and testing prior to deployment to production.	No exceptions noted.
		Inspected ticket details for a sample of changes selected from the ticketing system to determine changes were tested, peer reviewed and/or approved by management prior to implementation and were implemented by an individual separate from the approver.	No exceptions noted.
		Observed a user create a new branch without the required peer approval branch protections, and attempted to push a change from the new branch to production without the required approvals to determine the attempt was rejected by the deployment tool.	No exceptions noted.

Control Description	SOC 2 Criteria Reference	EY's Test Procedures	EY's Test Results
CM-05b: Standard Pre-Approved changes relate to low risk recurring changes that utilize established pre-approved templates.	<u>CC6.1</u> , <u>CC6.8</u> , <u>CC8.1</u>	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 ticket details for a sample of Standard Pre-Approved changes 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-08: A current asset inventory of production systems is documented and maintained.	<u>CC3.2</u> , <u>CC6.1</u> , <u>CC7.1</u>	Inspected the inventory list for production systems to determine a system inventory was available.	No exceptions noted.
CM-09: Documented configuration guidelines for the production environment govern the configuration management process.	<u>CC2.1</u> , <u>CC6.8</u> , <u>CC7.1</u> , <u>CC8.1</u>	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.	<u>CC6.8</u> , <u>CC7.1</u>	Inspected system configurations within the code repository to determine a centralized management tool was used to configure and manage production infrastructure.	No exceptions noted.
CM-14: The production server and container base image is rebuilt and made available once new vulnerabilities are identified in accordance with the Salesforce Vulnerability Ranking Standard.	<u>CC7.2</u>	Inspected Hyperforce documentation to determine process and requirements for container scanning and image bundle releases were defined.	No exceptions noted.
		Inspected system configurations to determine the production server base image was rebuilt and made available once new vulnerabilities were identified.	No exceptions noted.

Control Description	SOC 2 Criteria Reference	EY's Test Procedures	EY's Test Results
		Inspected the version history from the base image management console to determine new production server base images were made available monthly at a minimum.	No exceptions noted.
CP-01a: The Contingency Plan outlines the actions to be followed to meet availability and system requirements and is reviewed on an annual basis.	<u>CC7.4</u> , <u>CC7.5</u> , <u>CC9.1</u> , <u>A1.2</u>	Inspected the Contingency Plan documentation to determine it was reviewed each calendar year and outlined the actions to be followed in the event of a disaster to bring the production infrastructure back online to meet availability and system requirements, including the roles and responsibilities of each key personnel.	No exceptions noted.
CP-01b: 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.	<u>CC7.4</u> , <u>CC7.5</u> , <u>CC9.1</u> , <u>A1.2</u>	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 was reviewed within the past year.	No exceptions noted.
CP-04: Contingency documentation is communicated to individuals with contingency roles and responsibilities.	<u>CC1.4</u> , <u>CC2.2</u> , <u>CC7.5</u> , <u>CC9.1</u>	Inspected supporting evidence from company's extranet site to determine resiliency and failover documentation was communicated to individuals with contingency roles and responsibilities	No exceptions noted.
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.	<u>CC7.5</u> , <u>CC9.1</u> , <u>A1.2</u> , <u>A1.3</u>	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, results were reviewed, and corrective actions required were documented as necessary.	No exceptions noted.

Control Description	SOC 2 Criteria Reference	EY's Test Procedures	EY's Test Results
CP-06: The system is configured for high availability across multiple availability zones.	<u>CC7.5</u> , <u>CC9.1</u> , <u>A1.2</u> , <u>A1.3</u>	Inspected system configurations within the code repository and the management console to determine the system was configured for high availability across multiple availability zones.	No exceptions noted.
CP-07: Production systems are monitored for availability. Customer impacting performance incidents are documented in a ticketing system.	<u>CC9.1</u> , <u>A1.1</u>	Inspected the monitoring configuration in the centralized configuration management tool to determine production systems were monitored for availability.	No exceptions noted.
		Inspected the availability monitoring dashboard to determine production systems were monitored for availability.	No exceptions noted.
		Inspected the on-call monitoring schedule to determine on-call personnel were assigned for responding to alerts.	No exceptions noted.
		Inspected ticket details for a sample of performance incidents selected from the ticketing system to determine incidents were documented and tracked to resolution.	No exceptions noted.
CP-12: Database backups are performed and retained in accordance with the defined schedule in the backup procedures.	<u>CC9.1</u> , <u>A1.2</u> , <u>C1.1</u>	Inspected Salesforce's Database Backup Procedures and the Security, Privacy and Architecture documentation to determine requirements and procedures for performing system backups were documented.	No exceptions noted.
		Inspected the backup configurations within the code repository to determine backups were configured in accordance with the defined schedule and retention requirements.	No exceptions noted.

Control Description	SOC 2 Criteria Reference	EY's Test Procedures	EY's Test Results
		Inspected the backup monitoring configuration to determine the backup process was monitored and errors identified were requeued for resolution.	No exceptions noted.
IA-02: Privileged 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.	<u>CC6.1</u>	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.
IR-03: Incident handling capabilities for performance incidents have been implemented. Customer impacting performance incidents are assigned a severity level to prioritize their importance.	<u>CC2.1</u> , <u>CC5.1</u> , <u>CC5.3</u> , <u>CC7.4</u> , <u>CC7.5</u> , <u>CC8.1</u> , <u>CC9.1</u>	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 incident 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.

Control Description	SOC 2 Criteria Reference	EY's Test Procedures	EY's Test Results
IR-04: Investigation and corrective actions for customer impacting performance incidents are documented and shared with key personnel.	<u>CC5.1</u> , <u>CC5.2</u> , <u>CC7.3</u> , <u>CC7.4</u> , <u>CC7.5</u> , <u>CC9.1</u>	Inspected incident 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-02: Production container images stored in the container image registry are regularly scanned for vulnerabilities or after significant change.	<u>CC3.2</u> , <u>CC4.1</u> , <u>CC6.8</u> , <u>CC7.1</u> , <u>CC7.2</u>	Inspected the vulnerability scanner tool configurations to determine vulnerability scans were scheduled to run on a daily basis.	No exceptions noted.
		Inspected monitoring configurations to determine an alert was configured in the case of vulnerability scan failure.	No exceptions noted.
		Inspected log details within the centralized logging system to determine that production container images were regularly scanned for vulnerabilities.	No exceptions noted.
RA-06: Annually, Salesforce products complete infrastructure penetration testing for in-scope systems. Remediation of results are tracked to resolution.	<u>CC4.1</u>	Inspected Salesforce's Vulnerability Assessment and Identification Process and Vulnerability Ranking 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, if any, were tracked to resolution.	No exceptions noted.

Control Description	SOC 2 Criteria Reference	EY's Test Procedures	EY's Test Results
SC-03: Internal and external Domain Name Systems (DNS) are redundant and fault-tolerant.	<u>A1.1</u> , <u>A1.2</u>	Inspected configurations for a sample of internal and external Domain Name Systems selected from the asset inventory to determine they were redundant and fault tolerant.	No exceptions noted.
SC-06: Production and non-production environments are segregated.	<u>CC6.1</u> , <u>CC6.3</u> , <u>CC8.1</u>	Inspected network topology diagrams to determine production and non-production environments were segregated.	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-09: Sessions into the production infrastructure (network, servers, and database) and the application are automatically terminated after a period of inactivity and requires reauthentication.	<u>CC6.1</u>	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.
SC-10: Network traffic is protected and managed at external network connections by routing through boundary protection mechanisms.	<u>CC6.1</u> , <u>CC6.6</u>	Inspected network security policies and guidance documentation to determine boundary protection mechanisms were in place to manage inbound and outbound external connections.	No exceptions noted.
		Inspected system configurations for a sample of security groups within the code repository to determine they were configured to restrict access to the production environment.	No exceptions noted.

Control Description	SOC 2 Criteria Reference	EY's Test Procedures	EY's Test Results
SC-13: Customer Data is encrypted at rest.	CC6.1	Inspected system configurations within the code repository and the management console to determine production databases were configured to encrypt Customer Data at rest.	No exceptions noted.
SC-14: Classic cryptographic keys are rotated in accordance with the Cryptographic Key Management Standard.	CC6.1	Inspected Salesforce's Cryptographic Key Management Standard to determine it documented the requirements for managing and storing encryption keys and it was reviewed within the past year.	No exceptions noted.
		Inspected configurations within the code repository to determine encryption certificates were managed and stored in accordance with encryption key management policies and procedures, and included alerts in the event of expiring certificates.	No exceptions noted.
		Inspected a sample production environment to determine certificates were set to expire in accordance to the Cryptographic Key Management Standard.	No exceptions noted.
SC-15: Customer Data at rest encryption keys within the production environment are rotated in accordance with Salesforce Security Standards.	CC6.1	Inspected Salesforce's Cryptographic Key Management Standard to determine it documented the requirements for managing and storing encryption keys and it was reviewed within the past year.	No exceptions noted.
		Inspected configurations within the code repository and the management console to determine Customer Managed Keys (CMK) were managed using AWS's Key Management Services (KMS) and were configured to be rotated in accordance with policy.	No exceptions noted.

Control Description	SOC 2 Criteria Reference	EY's Test Procedures	EY's Test Results
SI-02: Salesforce utilizes an intrusion detection tool to monitor network traffic which generates alerts based on pre-defined definitions.	<u>CC6.6</u> , <u>CC6.8</u> , <u>CC7.1</u> , <u>CC7.2</u> , <u>CC7.4</u>	Inspected the configuration of the intrusion detection tool within the production environment to determine network traffic was monitored and logs were forwarded to the centralized logging system.	No exceptions noted.
		Inspected the centralized logging system for a sample event to determine the event was logged and an alert was generated based on pre-defined definitions.	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	<u>CP-04</u> Criteria is 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	<u>AU-02a</u> , <u>AU-02b</u> , <u>AU-03</u> , <u>AU-08</u> , <u>CM-02</u> , <u>CM-09</u> , <u>IR-03</u> Criteria is 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	<u>CP-04</u> Criteria is 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	Criteria 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.

Criteria	Controls list	Criteria
CC3.2	<u>CM-08</u> , <u>RA-02</u>	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.
CC3.3	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	<u>CM-01</u> , <u>RA-02</u> , <u>RA-06</u> Criteria is 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	<u>IR-03</u> , <u>IR-04</u> Criteria is 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	<u>AC-17</u> , <u>AU-02a</u> , <u>AU-02b</u> , <u>AU-08</u> , <u>IR-04</u> Criteria is 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	<u>AC-17</u> , <u>IR-03</u> Criteria is 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.

Criteria	Controls list	Criteria
CC 6.0 Common Criteria Related to Logical and Physical Access Controls		
CC6.1	<p>AC-05, AC-13a, AC-13b, AC-14, CM-05a, CM-05b, CM-08, IA-02, SC-06, SC-09, SC-10, SC-13, SC-14, SC-15</p> <p>Criteria is also addressed via subservice provider controls.</p>	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.
CC6.2	<p>AC-05, AC-13a, AC-13b, AC-14, AC-17, AC-18, AC-19, AC-22a, AC-22b, AC-22c</p> <p>Criteria is also addressed via subservice provider controls.</p>	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	<p>AC-05, AC-13a, AC-13b, AC-14, AC-17, SC-06</p> <p>Criteria is also addressed via subservice provider controls.</p>	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	<p>AC-22a, AC-22b, AC-22c, SC-10, SI-02</p> <p>Criteria is also addressed via subservice provider controls.</p>	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.
CC6.7	<p>AC-07</p> <p>Criteria is also addressed via subservice provider controls.</p>	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.

Criteria	Controls list	Criteria
CC6.8	<u>AC-07</u> , <u>CM-05a</u> , <u>CM-05b</u> , <u>CM-09</u> , <u>CM-13</u> , <u>RA-02</u> , <u>SI-02</u> Criteria is 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.

CC 7.0 Common Criteria Related to System Operations

CC7.1	<u>AC-05</u> , <u>CM-02</u> , <u>CM-08</u> , <u>CM-09</u> , <u>CM-13</u> , <u>RA-02</u> , <u>SI-02</u> Criteria is 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	<u>AU-02a</u> , <u>AU-02b</u> , <u>AU-03</u> , <u>AU-08</u> , <u>CM-14</u> , <u>RA-02</u> , <u>SI-02</u> Criteria is 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	<u>IR-04</u> Criteria is 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	<u>CP-01a</u> , <u>CP-01b</u> , <u>IR-03</u> , <u>IR-04</u> , <u>SI-02</u> Criteria is 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	<u>CM-01</u> , <u>CP-01a</u> , <u>CP-01b</u> , <u>CP-04</u> , <u>CP-05</u> , <u>CP-06</u> , <u>IR-03</u> , <u>IR-04</u> Criteria is 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	<u>CM-02</u> , <u>CM-05a</u> , <u>CM-05b</u> , <u>CM-09</u> , <u>IR-03</u> , <u>SC-06</u> Criteria is 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.
-------	---	--

Criteria	Controls list	Criteria
CC 9.0 Common Criteria Related to Risk Mitigation		
CC9.1	<u>CP-01a</u> , <u>CP-01b</u> , <u>CP-04</u> , <u>CP-05</u> , <u>CP-06</u> , <u>CP-07</u> , <u>CP-12</u> , <u>IR-03</u> , <u>IR-04</u> Criteria is also addressed via subservice provider controls.	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.
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	<u>CM-01</u> , <u>CP-07</u> , <u>SC-03</u> Criteria is 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	<u>CP-01a</u> , <u>CP-01b</u> , <u>CP-05</u> , <u>CP-06</u> , <u>CP-12</u> , <u>SC-03</u> Criteria is 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	<u>CP-05</u> , <u>CP-06</u> Criteria is 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	<u>CP-12</u> Criteria is also addressed via subservice provider controls.	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.
C1.2	Criteria addressed via subservice provider controls.	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.