



Fusion Risk Management, Inc.

System and Organization Controls (“SOC”) for
Service Organizations Report 2, Type 2
(SOC 2®, Type 2)

*Report on Fusion Risk Management’s Description of its Fusion Framework® System™
and the Suitability of the Design and Operating Effectiveness of Controls Relevant to
Security*

For the period July 1, 2020 to June 30, 2021



Confidential Material

Unauthorized use, reproduction, or distribution of this report, in whole or in part, is strictly prohibited.

TABLE OF CONTENTS

Section 1: Fusion Risk Management’s Assertion.....	1
Section 2: Independent Service Auditor’s Report.....	4
Section 3: Fusion Risk Management’s Description of Its Fusion Framework® System™ .	11
Company Background and Services Provided	12
Principal Service Commitments and System Requirements	12
Components of the Fusion Framework® System™	13
Infrastructure.....	15
Software	16
People	19
Procedures	20
Data.....	21
System Incidents.....	22
Applicable Trust Services Criteria and Related Controls	22
Applicable Trust Services Criteria.....	22
Relevant Aspects of the Control Environment, Risk Assessment Process, Information and Communication, Monitoring Activities, and Control Activities	22
Complementary User-Entity Controls	26
Subservice Organizations	28
Services Provided and Applicable Trust Services Criteria.....	28
Complementary Subservice Organization Controls	32
Significant Changes During the SOC 2® Period	34
COVID-19 Response.....	34
Section 4: Trust Services Criteria, Related Controls, and FG MK’s Tests of Controls.....	35
Security (Common Criteria)	36
Section 5: Other Information Provided by Fusion	94
Fusion Management’s Responses to FG MK Testing Exceptions.....	95

Section 1

Fusion Risk Management's Assertion

MANAGEMENT'S ASSERTION

We have prepared the accompanying description in Section 3 of Fusion Risk Management, Inc.'s ("Fusion") system titled "Fusion's Description of Its Fusion Framework® System™" throughout the period July 1, 2020 to June 30, 2021 (description) based on the criteria for a description of a service organization's system set forth in DC 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*). The description is intended to provide report users with information about the Fusion Framework® system that may be useful when assessing the risks arising from interactions with Fusion's system, particularly information about system controls that Fusion has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Fusion uses subservice organizations to 1) provide cloud hosting services; 2) provide single sign-on services; 3) provide document rendering services; and 4) provide office workspace hosting services (for Fusion's London, England location). The description indicates that complementary subservice organization controls are suitably designed and operating effectively are necessary, along with controls at Fusion, to achieve Fusion's service commitments and system requirements based on the applicable trust services criteria. The description presents Fusion's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Fusion's controls. The description does not disclose the actual controls at the subservice organizations.

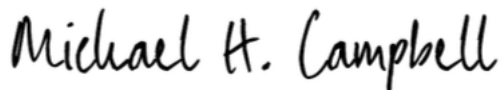
The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Fusion, to achieve Fusion's service commitments and system requirements based on the applicable trust services criteria. The description presents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

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

- 1) The description presents Fusion's Fusion Framework® system that was designed and implemented throughout the period July 1, 2020 to June 30, 2021 in accordance with the description criteria.
- 2) The controls stated in the description were suitably designed throughout the period July 1, 2020 to June 30, 2021 to provide reasonable assurance that Fusion's service commitments and system requirements would be

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

- 3) The controls stated in the description operated effectively throughout the period July 1, 2020 to June 30, 2021 to provide reasonable assurance that Fusion's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Fusion's controls operated effectively throughout that period.



Michael Campbell
Chief Executive Officer



James Stewart
Chief Financial Officer

Section 2

Independent Service Auditor's Report

Independent Service Auditor's Report

To the Management of Fusion Risk Management, Inc. ("Fusion" or "Company")
Chicago, Illinois

Scope

We have examined Fusion's accompanying description of its Fusion Framework® System™ found in Section 3 titled Fusion Risk Management's Description of Its Fusion Framework® System™ throughout the period July 1, 2020 to June 30, 2021 (description) based on the criteria for a description of a service organization's system set forth in DC 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period July 1, 2020 to June 30, 2021, to provide reasonable assurance that Fusion's service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

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

Fusion uses subservice organizations to provide: 1) cloud hosting services; 2) single sign-on services; 3) document rendering services; and 4) office workspace hosting services (for Fusion's London, England

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

The information in Section 5, titled "Other Information Provided by Fusion", describes the service organization's responses to FGMK's testing exceptions noted. It is presented by management of Fusion to provide additional information and is not a part of the service organization's description of its Fusion Framework® System™ made available to user entities during the period July 1, 2020 to June 30, 2021. Information in Section 5, titled "Other Information Provided by Fusion" has not been subjected to the procedures applied in the examination of the description of the Fusion Framework® System™ and the suitability of the design and operating effectiveness of controls to meet the related trust services criteria identified in the description of the Fusion Framework® System™. Accordingly, we do not express an opinion on the fairness of the presentation of the information in Section 5, titled "Other Information Provided by Fusion", or on the suitability of the design and operating effectiveness of controls related to that information.

Service Organization's Responsibilities

Fusion 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 Fusion's service commitments and system requirements were achieved. In Section 1, Fusion has provided the accompanying assertion titled "Fusion Risk Management's Assertion" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Fusion is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the

description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

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

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

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

- testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- evaluating the overall presentation of the description.

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs. There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design or operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are listed in Section 4, "Trust Services Criteria, Related Controls, and FGМК's Tests of Controls" of this report.

Opinion

In our opinion, in all material respects:

- a. the description presents Fusion's Fusion Framework® System™ that was designed and implemented throughout the period July 1, 2020 to June 30, 2021 in accordance with the description criteria.

- b. the controls stated in the description were suitably designed throughout the period July 1, 2020 to June 30, 2021 to provide reasonable assurance that Fusion's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organizations and user entities applied the complementary controls assumed in the design of Fusion's controls throughout that period.
- c. the controls stated in the description operated effectively throughout the period July 1, 2020 to June 30, 2021 to provide reasonable assurance that Fusion's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complimentary user entity controls assumed in the design of Fusion's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of Fusion ; user entities of Fusion 's Fusion Framework® System™ during some or all of the period July 1, 2020 to June 30, 2021 , business partners of Fusion subject to risks arising from interactions with the Fusion Framework® System™, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

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

- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

This report is not intended to be, and should not be, used by anyone other than the specified parties.

FGMK, LLC

Chicago, Illinois

December 13, 2021

Section 3

Fusion Risk Management's Description of Its
Fusion Framework[®] System[™]

Fusion Risk Management's Description of Its Fusion Framework® System™

Company Background and Services Provided

Founded in 2006 by David Nolan, Vic Fricas, John Jackson, and Bob Sibik, Fusion Risk Management, Inc. ("Fusion", "Fusion RM", or the "Company") operates out of offices in Rolling Meadows, Illinois; Chicago, Illinois; and London, England.

In September 2019, Vista Equity Partners acquired a majority ownership stake in Fusion, with both current investors, Catalyst Investors and Level Equity, maintaining minority ownership stakes in the Company.

Fusion provides organizations globally with business continuity and risk management solutions. Fusion's custom-developed, proprietary Fusion Framework® System™ is delivered within the Salesforce, Inc. ("Salesforce") Lightning Platform and is designed to adapt and evolve with its customers' businesses. Fusion also provides technical and advisory consulting services to assist its customers deriving maximum value from their investment in the Fusion Framework® System™. Fusion's technical consultants tailor the Fusion Framework® System™ to each customer's needs while Fusion's advisory consultants help customers establish or refine their business continuity and risk programs.

Principal Service Commitments and System Requirements

Fusion management designs and implements its processes and procedures related to its Fusion Framework® System™ to meet its services objectives. Those objectives are based on the service commitments that Fusion makes to its user entities, the applicable laws and regulations that govern the Fusion Framework® System™ and services, and the operational and compliance requirements that Fusion has established for its Fusion Framework® System™.

Security commitments to customers are documented and communicated as part of each customer's Master Services Agreement ("MSA") and Statement of Work ("SOW"). The Fusion Framework® System™ security commitments to Fusion's customers include, but are not limited to, the following:

- logical access to Fusion Framework® System™ components (infrastructure, software, people, procedures, and data as identified below) is restricted to authorized Fusion personnel and vendors (if necessary) as needed to perform their job responsibilities;
- physical access to Fusion Framework® System™ components within Fusion's control is restricted to authorized Fusion personnel and vendors (if necessary) as needed to perform their job responsibilities.

Components of the Fusion Framework® System™

Fusion has designed and implemented the Fusion Framework® System™ to operate within the salesforce.com Lightning Platform (formerly known as Force.com). The Fusion Framework® System™ was designed to enable Fusion's customers to take over full operation and administration subsequent to Fusion's implementation or allow Fusion's customers to leverage Fusion's consulting and support services as needed.

Each Fusion customer has their own custom-configured instance within the Lightning Platform. This instance, also called an organization ("Org" for short), is unique to each Fusion customer while at the same time leveraging the proprietary design, content, tools, and configurations developed by Fusion.

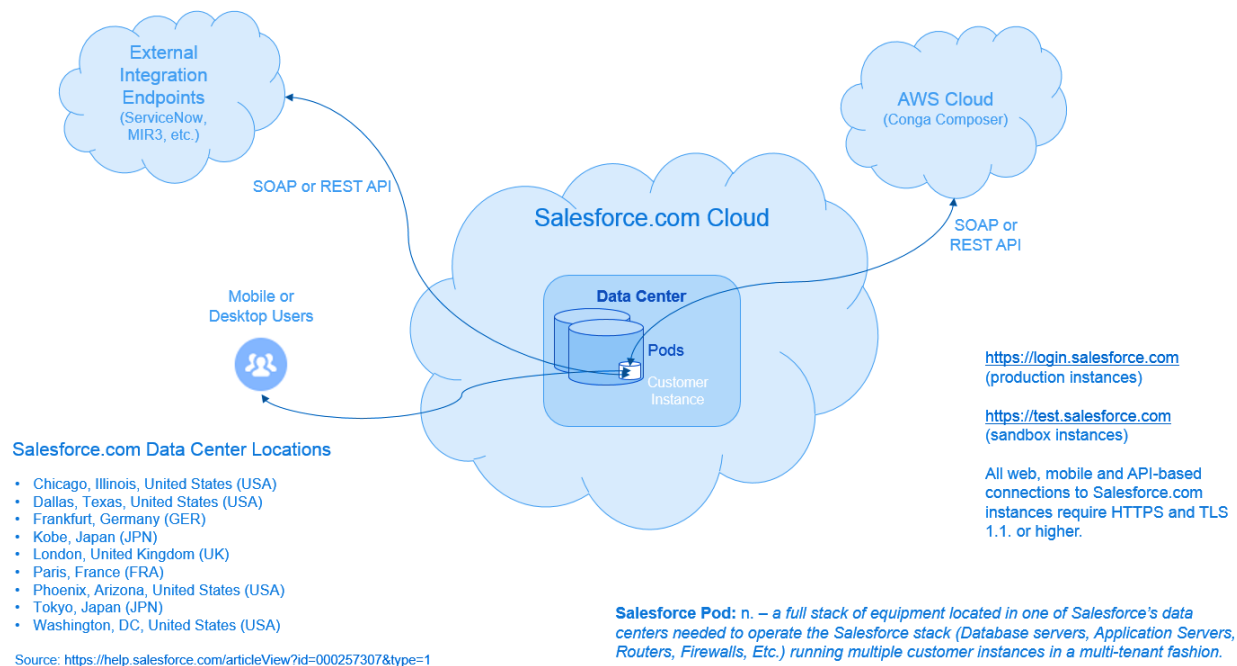
The Fusion Framework® System™ is comprised of the key components as described in the sections below, organized according to the following definition of system in the context of a SOC 2® report per the American Institute of Certified Public Accountants ("AICPA"):

- Infrastructure: Disclosures about the collection of physical or virtual resources that supports an overall IT environment, including the physical environment and related structures, IT, and related hardware (for example, facilities, servers, storage, environmental monitoring equipment, data storage devices and media, mobile devices, and internal networks and

connected external telecommunications networks) that the service organization uses to provide the services.

- Software: Disclosures about the application programs, the IT system software that supports those application programs (operating systems, middleware, and utilities), the types of databases used, the nature of external-facing web applications, and the nature of applications developed in-house, including details about whether the applications in use are mobile applications or desktop and laptop applications.
- People: Disclosures about the personnel involved in the governance, management, operation, security, and use of the system (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers).
- Procedures: Disclosures about the automated and manual procedures implemented by the service organization primarily relate to those through which services are provided. These include, as appropriate, procedures through which service activities are initiated, authorized, performed, and delivered, and reports and other information prepared.
- Data: Disclosures about the types of data used by the system, transaction streams, files, databases, tables, and output used or processed by the system.

The diagram below provides an overview of the Fusion Framework® System™, following by further description of the various locations and components.



Infrastructure

Fusion personnel (employees and contractors) are based out of the Rolling Meadows, Illinois; Chicago, Illinois; and London, England offices, which serve as the locations for the management, development, operations and sales/marketing teams. The in-scope hardware components within the Rolling Meadows and Chicago Fusion office locations consist of industry standard servers, workstations and networking devices (e.g., routers, firewalls, switches). Fusion is responsible for the implementation and maintenance of the hardware components at the Rolling Meadows and Chicago offices. The Fusion London office is a shared office space and in-scope system hardware components include Fusion workstations.

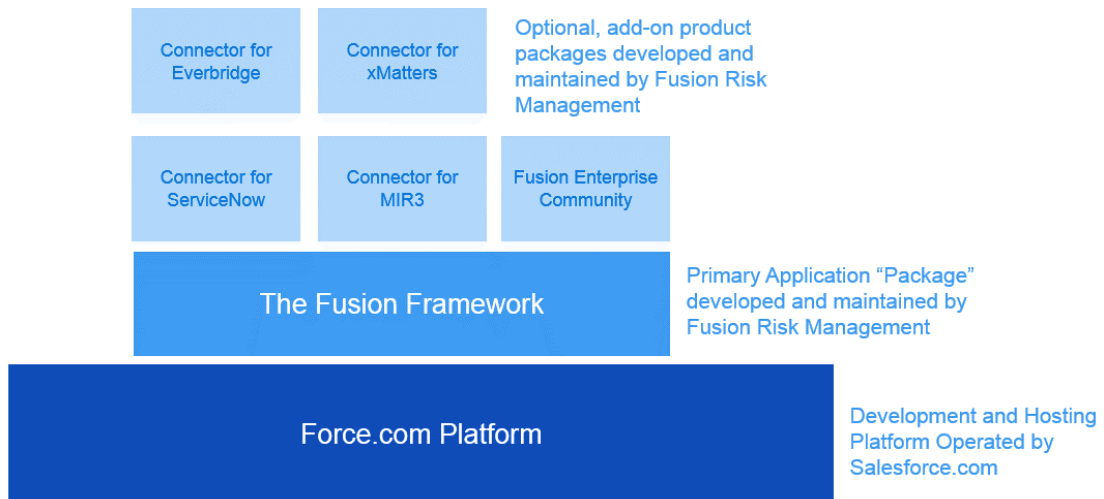
The production environment for the Fusion Framework® System™ is located within the Salesforce.com cloud platform. Fusion relies on Salesforce.com to provide the hardware and software within the Lightning Platform environment as needed to support the requirements of the Fusion Framework® System™. The production hardware at Salesforce.com is distributed for redundancy purposes throughout various Salesforce.com data centers globally, with each data center hosting many “Salesforce Pods”. Each

Salesforce Pod is comprised of the hardware (servers, firewalls, routers, etc.) needed to support a customer instance, with multiple Salesforce customers sharing the same Salesforce Pod, separated by logical security. Salesforce is responsible for the design, implementation and maintenance of the hardware components at its global data centers.

Software

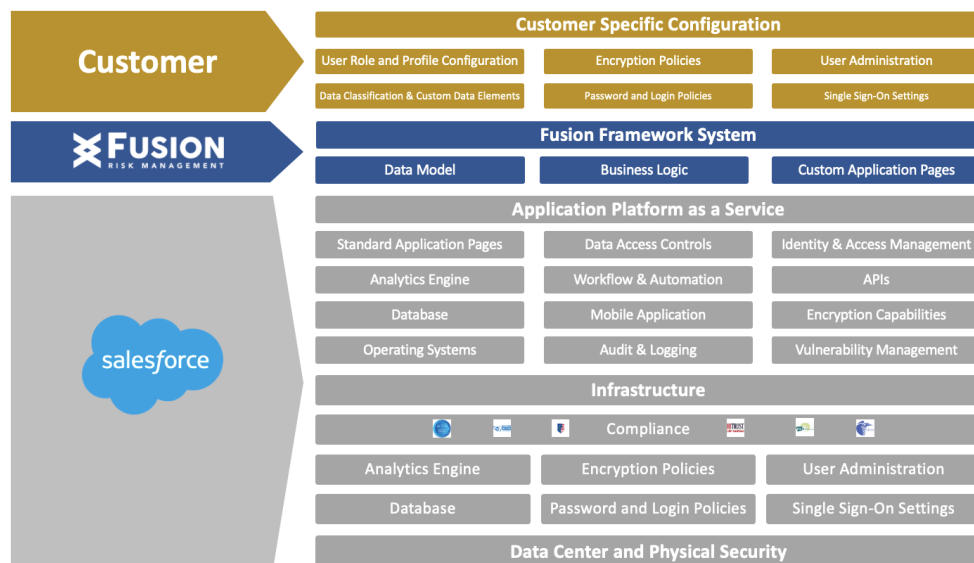
Each Fusion customer instance, or Org, within the Salesforce.com production environment is comprised of the following software layers and components:

Salesforce.com Customer Instance



Note: "Force.com Platform" or "Force.com" (as presented in the diagram above and throughout this report) is used interchangeably with "Lightning Platform" or "Lightning" as Salesforce is in process of rebranding the name "Force.com Platform" / "Force.com" to "Lightning Platform" / "Lightning".

Also, the following diagram depicts the shared responsibility framework that Fusion has identified for the Salesforce environment.



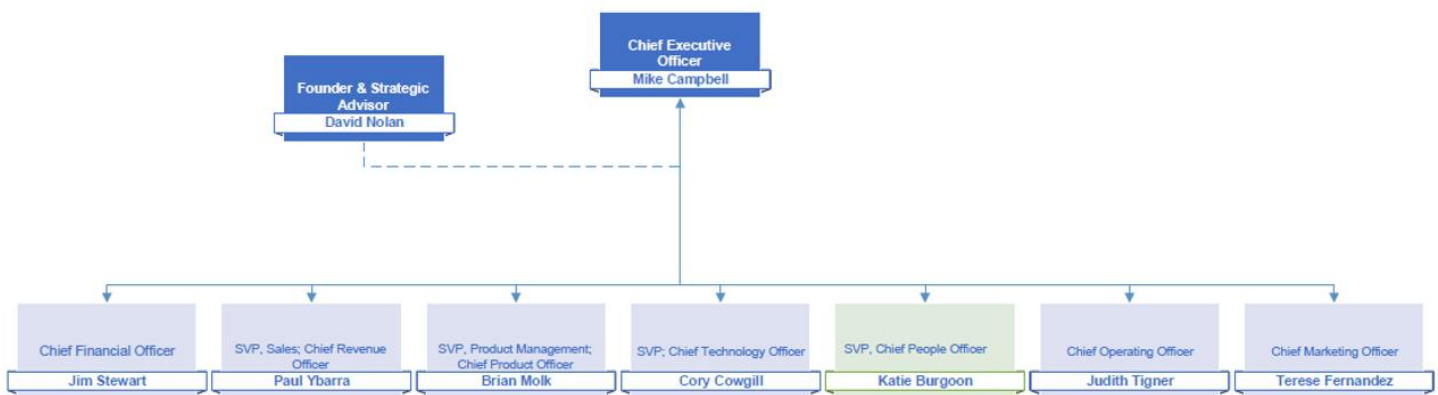
The Fusion Framework® System™ is implemented within Salesforce’s Lightning Platform. Salesforce is responsible for the development, operation and maintenance of the Lightning Platform environment, while Fusion is responsible for the development, operation, and maintenance of the Fusion Framework® System™ software components as presented above the “Force.com Platform” blue box in the diagram above.

In addition to the software components described above, Fusion has implemented the following operating systems, middleware, and utilities to support its technology infrastructure located at the Chicago and Rolling Meadows locations.

Software	Vendor	Description / Purpose
Insight VM & IDR	Rapid7 LLC	For network and vulnerability scanning (malicious software, unauthorized changes to system files, admin logins, user logins, firewall log review) at the Rolling Meadows and Chicago offices
Jira	Atlassian, Inc.	For help desk/change management logging and tracking
Sophos Endpoint Protection	Sophos Ltd.	For servers and workstations at the Rolling Meadows, Chicago, and London offices
Sophos SG UTM	Sophos Ltd.	Firewalls at the Rolling Meadows and Chicago offices
MS Active Directory	Microsoft Corporation	To authenticate and authorize Fusion personnel and computers
MS Windows OS	Microsoft Corporation	Operating system for servers and selected workstations at the Rolling Meadows, Chicago, and London offices
macOS	Apple Inc.	Operating system for selected workstations at the Rolling Meadows, Chicago, and London offices
Okta	Okta, Inc.	Single sign-on to allow Fusion personnel to access the Fusion Framework® System™ component at Salesforce
Conga Composer	AppExtremes, LLC	Renders documents/reports from the Fusion Framework® System™ data at Salesforce

People

Fusion RM has a team of over 170 employees that are based in the Chicago and Rolling Meadows offices. The leadership team is primarily located in the Chicago office, while the Rolling Meadows office is home for selected development, product marketing and back office functions. The organization and reporting lines of the Fusion RM leadership team is presented in the following diagram, followed by a description of each key area that is relevant to security of the Fusion Framework® System™.



Operations and Service Delivery

Judith Tigner, COO, has oversight for Professional Services and Support Operations of the Fusion Framework® System™. Paul Ybarra, CRO, is responsible for customers account management. Jim Stewart, CFO, is responsible for the development and implementation of Fusion's overall policies and procedures, compliance, and administrative technology at the Chicago and Rolling Meadows offices. Cory Cowgill, CTO, is responsible for Fusion's information security management program as well as the technical architecture and product engineering operations for the Fusion Framework® System™.

Product Management

Brian Molk leads Product Management and is responsible for leading the effort to continuously enhance the Fusion Framework® System™ features and functions to provide an effective platform to manage business continuity and risk. In order to accomplish this, the product management team tracks current industry trends, Fusion customers' evolving business continuity requirements, and relevant Lightning Platform enhancements. Product management synthesizes these three inputs and creates a multi-year product roadmap detailing future product enhancements. The Fusion Framework® System™ undergoes two major product enhancement releases per year.

Human Resources

The Human Resources ("HR") department is directed by Katie Burgoon, who oversees the recruiting, screening, interviewing, hiring, onboarding, and development of new employees. Katie works with Fusion management to ensure compliance with the Company's established hiring practices designed to identify people that have the requisite skills and experience to satisfy specific job functions. Katie also is responsible for ensuring that new hires are subjected to background checks, that they sign-off on the employee handbook and other relevant Company policies and procedures, and that they attend training (including security awareness training) upon hire, and then annually.

Procedures

Fusion management understands the importance of the proper design, development and implementation of automated and manual procedures to support security of Fusion Framework® System™ components. As such, Fusion management has documented and implemented the following policies and procedures that are relevant to security:

- Information Security
- Organization of Information Security
- Human Resources Security
- Asset Management
- Access Control
- Physical and Environment Security
- Operations Security
- Communications Security
- Information Security Incident Management
- Acceptable Use

Data

The data tables that are integral to the operation of the Fusion Framework® System™ are instantiated as Lightning Platform objects (data tables and meta data) and are linked together to establish the data relationships relevant to managing business continuity and risk. These data tables may contain thousands of fields relevant to each customer's instance of the Fusion Framework® System™. Examples of data typically captured in the Fusion Framework® System™ include information on:

- | | | |
|-----------------|----------------------|-------------------------------|
| ➤ Facilities | ➤ Components | ➤ Vendors |
| ➤ Processes | ➤ Incidents | ➤ Teams |
| ➤ Applications | ➤ Employees | ➤ Rosters |
| ➤ BC Plan Steps | ➤ BC Plan Procedures | ➤ Risks, Threats and Controls |

System Incidents

There were no identified system incidents related to Fusion's controls that: a) were the result of controls that were not suitably designed or operating effectively; or b) otherwise resulted in a significant failure in the achievement of one or more of the service commitments and system requirements specified in this description of the Fusion Framework® System™ for the period covered by this system description.

Applicable Trust Services Criteria and Related Controls

Applicable Trust Services Criteria

The trust services criteria for the security category (applicable trust services criteria) were used to evaluate the suitability of design and operating effectiveness of controls stated in this system description. The security criteria and related controls are designed to ensure that:

- information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet its objectives.

The applicable trust services criteria presented in Section 4 ("Trust Services Criteria, Related Controls, and FGMK's Tests of Controls") of this report are an integral part of Fusion's system description.

Relevant Aspects of the Control Environment, Risk Assessment Process, Information and Communication, Monitoring Activities, and Control Activities

Fusion management understands the importance of an internal control system to help keep Fusion stay focused on its core initiatives and operations, and for the ongoing security of the Fusion Framework® System™. As such, Fusion management has designed and implemented the following internal control components that it deems relevant to the security of the Fusion Framework® System™.

Control Environment

Fusion management considers the following areas to be important and relevant to maintaining an effective control environment.

Management Philosophy Operating Style

Fusion management understands that an effective control environment begins at the top and then permeates throughout the organization. Fusion management consistently communicates the importance of internal controls during daily activities and Company meetings. Fusion management has established processes and procedures designed to ensure that information relevant to the Fusion Framework® System™ remains secure over time.

Human Resource Policies

Fusion employees are the key resources underlying service delivery standards set by Fusion management. As such, Fusion management has implemented hiring policies and practices to ensure that new employees possess the skills, experience and ethical behavior traits that align with Fusion management's goals and business strategy.

The following are some of the human resource policies implemented by Fusion management to achieve its goals:

- Fusion policy requires background checks and drug testing for any individual to be initiated prior to employment start date.
- New employees are required to be interviewed by HR, management, and peer(s) according to criteria per job description.
- New Fusion employees and those with significant changes in role are required to be trained according to their training plan.
- Fusion employees are required to acknowledge in writing within their first week of employment that they are responsible for reading and understanding the Fusion Employee

Handbook, which includes, but is not limited to, responsibilities for keeping Company and customer information confidential and compliance with Fusion policies and procedures.

- Fusion personnel are required to acknowledge in writing that they have completed Fusion's Security Awareness Training webinar upon hire and annually thereafter.

Organizational Structure

Fusion management has established an organizational structure that clearly established reporting lines and areas of responsibilities. Each department head has further organized their department to assign specific functions to managers and their supporting personnel. At all levels, Fusion personnel are held accountable for their specific responsibilities as well as the actions of their managed personnel, when reasonable. See section "People" above for additional information related to organizational structure.

Risk Assessment Process

Fusion management created the Fusion Information Security Management Group to establish and manage the risk assessment process, which includes identification and management of internal and external risks. Also, Fusion has engaged a third-party security consultant as its virtual Chief Information Security Officer ("CISO") and meets with the CISO weekly. The Company uses a risk register to log and track relevant risks and manage the corresponding risk treatment plans.

Information and Communication

Fusion management understands the high importance of effective communications with employees and customers as a means to carry out its businesses services and maintain adequate internal control. Fusion leverages the Salesforce's Case Management Software to allow its customers to submit service and change requests, and then to track the progress of those requests. Internally, Fusion relies on third-party tools such as Atlassian's Jira to log and track change requests.

Fusion also has an intranet site that is used to communicate diverse topics and serves as the repository for Fusion's formally documented policies and procedures that convey management's intentions and strategies relating to Fusion Framework® System™ security.

Monitoring Activities

Fusion management has overall responsibility for Fusion Framework® System™ controls and has implemented the Fusion Information Security Management Group to oversee and monitor the design and operation of those controls. Also, Fusion management has implemented third-party and custom developed tools to deliver the information needed to operate, maintain, and monitor the Fusion Framework® System™ and give management the controls necessary to achieve customer commitments.

Control Activities

The applicable control activities presented in Section 4 (“Trust Services Criteria, Related Controls, and FGМК’s Tests of Controls”) are an integral part of Fusion's system description.

Complementary User-Entity Controls

Fusion's services and related controls were designed with the assumption that certain controls will be implemented by user-entities. Such controls, called complementary user-entity controls, should be in operation at the user-entity to complement Fusion's controls. User-entities of the Fusion Framework® System™ should maintain controls to provide reasonable assurance that:

1. Fusion RM customers have controls to provide reasonable assurance that Fusion Framework® System™ user accounts that are no longer needed are removed, or the customer notifies Fusion to remove them.
2. Fusion RM customers have controls to provide reasonable assurance that user access requests for Fusion support are authorized prior to access being granted to the customer's Org.
3. Fusion RM customers have controls to provide reasonable assurance that user accounts setup by the customer for Fusion personnel for access to the customers' respective Orgs on the Lightning Platform are configured for appropriate multi-factor authentication (e.g., using a Fusion email account).
4. Fusion RM customers have controls to provide reasonable assurance that all user access (including administrator access) is periodically reviewed to ensure that all users remain authorized and continue to only have access to Fusion Framework® System™ functions and data as required, disabling any unauthorized accounts, and notifying Fusion of any unauthorized accounts for which customer is uncertain of its origin.
5. Fusion RM customers have controls to provide reasonable assurance that changes implemented by the customer to their instance of the Fusion Framework® System™ follow changes controls to ensure that changes do not adversely affect Fusion Framework® System™ security.
6. Fusion RM customers have controls to provide reasonable assurance that their personnel are notified of new responsibilities relating to changes to the Fusion Framework® System™ that were implemented by the customer administrator or by Fusion RM.

7. Fusion RM customers have controls to provide reasonable assurance that initial setup of user authentication settings including but not limited to password complexity, IP whitelisting, single sign-on, and two-factor authentication, for their respective Orgs on the Lightning Platform is reviewed and approved.
8. Fusion RM customers have controls to provide reasonable assurance that setup of user authentication settings including but not limited to password complexity, IP whitelisting, single sign-on, and two-factor authentication, for their respective Orgs on the Lightning Platform is periodically reviewed and either updated according to current requirements or request are made for Fusion RM to update.
9. Fusion RM customers have controls to provide reasonable assurance that mobile device access settings for their Org on the Lightning Platform are setup and maintained according to current requirements or requesting Fusion RM to update according to current requirements.
10. Fusion RM customers have controls to provide reasonable assurance that security for their data in the Fusion Framework® System™ and the data encryption policies via Salesforce Classic / Shield Encryption in accordance with the customers' data classification is configured (or directing Fusion to configure) according to customers' policy.

Subservice Organizations

Services Provided and Applicable Trust Services Criteria

Fusion utilizes subservice organizations, as described below, to perform functions that support certain Fusion services and operation of the Fusion Framework® System™. The description in Section 3 of this report includes only the policies, procedures, and control activities at Fusion, and does not include the policies, procedures, and control activities at these third-party service organizations. Also, the examination by the Independent Service Auditors does not extend to the policies, procedures, and control activities at these third-party subservice organizations.

The applicable trust services criteria that are intended to be met by controls at the subservice organizations in combination with controls at Fusion are as follows:

Subservice Organization	Services Provided	Applicable Trust Services Criteria
Salesforce.com, Inc. ("Salesforce")	Provides the Lightning Platform hosting services for the cloud production environment.	<p>CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.</p> <p>CC6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.</p> <p>CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.</p> <p>CC7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.</p> <p>CC7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.</p> <p>CC8.1 The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.</p>

Subservice Organization	Services Provided	Applicable Trust Services Criteria
Okta, Inc. ("Okta")	Provides single sign-on software as service ("SaaS") to allow Fusion personnel to access the Fusion Framework® System™ component at Salesforce	<p>CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.</p> <p>CC6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.</p>
AppExtremes, LLC ("AppExtremes")	Provides document rendering SaaS (Conga Composer) using Fusion Framework® System™ production data	<p>CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.</p> <p>CC7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.</p> <p>CC7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.</p> <p>CC8.1 The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.</p>

Subservice Organization	Services Provided	Applicable Trust Services Criteria
WeWork	Provides workspace for Fusion's London, England office	<p>CC6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.</p> <p>CC7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.</p>

Complementary Subservice Organization Controls

The following list includes the types of controls that Fusion management assumed, in the design of the Fusion Framework® System™, would be implemented by the subservice organizations and are necessary, in combination with controls at Fusion, to provide reasonable assurance that Fusion's service commitments and system requirements relevant to security are achieved.

Applicable Trust Services Criteria	Type of Controls Expected at the Subservice Organizations	Relevant Subservice Organizations
CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Logical access is approved, removed when no longer required, and periodically reviewed to ensure it remains authorized over time.	Salesforce Okta AppExtremes
CC6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	Physical access is approved, removed when no longer required, and periodically reviewed to ensure it remains authorized over time.	Salesforce WeWork
CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	System monitoring tools are implemented, and alerts are addressed timely as deemed appropriate based on the severity.	Salesforce Okta AppExtremes
CC7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Personnel respond timely as deemed appropriate based on the severity of potential security events according to defined incident management procedures.	Salesforce Okta AppExtremes WeWork
CC8.1 The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	System changes are authorized, tested, and approved for implementation in the production environment.	Salesforce Okta AppExtremes

Significant Changes During the SOC 2® Period

COVID-19 Response

Fusion began monitoring the COVID-19 pandemic starting in January 2020. Fusion activated its pandemic plan in March 2020. As such, there was no significant impact to Fusion's business operations or the ability for Fusion to meet its obligations to customer (e.g., security of the Fusion Framework® System™). An executive summary of the actions taken by Fusion is available upon customer request.

Section 4

Trust Services Criteria, Related Controls, and
FGMK's Tests of Controls

Trust Services Criteria, Related Controls, and FGМК's Tests of Controls

Security (Common Criteria)

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

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

CC1.0: CONTROL ENVIRONMENT			
CNTL #	Description of Fusion's Controls	FGМК's Tests of Controls	Results of FGМК's Tests of Controls
CC1.1	<i>COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.</i>		
CC1.1-01	Fusion Risk Management, Inc. ("Fusion" or "Company") senior management has established the Fusion Employee Handbook and Employment Agreement, and Contractor Agreement that sets expectations for conduct as well as confidentiality of Company and customer information.	Inquired of Fusion management and inspected the current Fusion Employee Handbook, Employment Agreement, and Contractor Agreement to determine that they set expectations for conduct as well as confidentiality of Company and customer information.	No exceptions noted.
CC1.1-02	Fusion personnel (full-time employees, part-time employees, and interns) are required to acknowledge in writing within their first week of employment that they	For a sample of new personnel, inquired of Fusion management and inspected the Fusion Employee Handbook acknowledgement forms to determine that	No exceptions noted.

CC1.0: CONTROL ENVIRONMENT

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
	are responsible for reading and understanding the Fusion Employee Handbook.	the Fusion Employee Handbook was acknowledged in writing within the first week of employment.	
CC1.1-03	Fusion personnel are required to report any known violation of the Company's policies, including inappropriate business conduct, to their manager. Fusion managers are required to address any of these issues reported to them and notify HR as deemed necessary.	Inquired of Fusion management and inspected the performance improvement program report and correspondence from Fusion management to determine that Fusion personnel reported any known violation of the Company's policies, including inappropriate business conduct, to their manager, a Fusion manager addressed the only issues reported to them during the SOC 2® period, and HR was notified as deemed necessary.	No exceptions noted.
CC1.1-04	For Fusion vendors that require their employees to have logical or physical access to Fusion Framework® System™ components, Fusion management assigns a Fusion employee to monitor and oversee the vendor employee's activities.	For a sample of new vendor employees that required logical or physical access to a Fusion Framework® System™ component, inquired of Fusion management and inspected the vendor MSA, SOW, or the vendor employee profile to determine that Fusion management assigned a Fusion employee to monitor and oversee the vendor employee's activities.	No exceptions noted.
CC1.1-05	Disciplinary action up to and including termination of employment is taken for violation of the Company's policies.	Inquired of Fusion management and inspected the performance improvement program report and correspondence from Fusion management to determine that disciplinary action up to and including termination of employment was taken for violation of the Company's policies.	No exceptions noted.

CC1.0: CONTROL ENVIRONMENT

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
CC1.2	<i>COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.</i>		
CC1.2-01	The Fusion board of directors ("BoD") is aware, and agrees that Fusion senior management has overall responsibility for Fusion Framework® System™ security. The CEO and CFO are on the BoD, and either informs the BoD of significant issues, if any, related to Fusion Framework® System™ security.	Inquired of Fusion management and inspected the BoD meeting minutes to determine that the Fusion BoD was aware, and agreed that Fusion senior management had overall responsibility for Fusion Framework® System™ security, the CEO and CFO were on the BoD, and they informed the BoD of that there were no significant issues related to Fusion Framework® System™ security.	No exceptions noted.
CC1.2-02	The Fusion BoD takes appropriate, relevant, and independent action based on significant issues, if any, related to Fusion Framework® System™ security as reported by the CEO or the CFO.	Inquired of Fusion management and inspected the BoD meeting minutes to determine that there were no significant issues related to Fusion Framework® System™ security reported to the BoD by the CEO or the CFO during the SOC 2® period.	FGMK was not able to test operating effectiveness of this control as there were no significant issues related to Fusion Framework® System™ security reported to the BoD by the CEO or the CFO during the SOC 2® period.
CC1.2-03	Fusion engages third-party security consultants if necessary, to address Fusion Framework® System™ security requirements that are not fulfilled by current Fusion personnel.	Inquired of Fusion management and inspected the current vCISO agreement to determine that Fusion engaged a third-party security consultant to address Fusion Framework® System™ security requirements that were not fulfilled by current Fusion personnel.	No exceptions noted.
CC1.3	<i>COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.</i>		

CC1.0: CONTROL ENVIRONMENT

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
CC1.3-01	The Fusion board of directors ("BoD") is aware, and agrees that Fusion senior management has overall responsibility for Fusion Framework® System™ security. The CEO and CFO are on the BoD, and either informs the BoD of significant issues, if any, related to Fusion Framework® System™ security.	Inquired of Fusion management and inspected the BoD meeting minutes to determine that the Fusion BoD was aware, and agreed that Fusion senior management had overall responsibility for Fusion Framework® System™ security, the CEO and CFO were on the BoD, and they informed the BoD of that there were no significant issues related to Fusion Framework® System™ security.	No exceptions noted.
CC1.3-02	Fusion senior management has established an organizational structure that includes authorities, responsibilities and reporting lines relating to Fusion Framework® System™ security.	Inquired of Fusion management and inspected the current organization chart to determine that Fusion senior management established an organizational structure that included authorities, responsibilities and reporting lines relating to Fusion Framework® System™ security.	No exceptions noted.
CC1.3-03	Fusion senior management has established the Fusion Information Security Management Team to assist with the achievement of Fusion Framework® System™ security objectives.	For a sample of weeks, inquired of Fusion management and inspected the current risk register and the minutes from the Fusion Information Security Management Team meetings with the vCISO to determine that Fusion senior management established the Fusion Information Security Management Team to assist with the achievement of Fusion Framework® System™ security objectives.	No exceptions noted.
CC1.3-04	Fusion contractors that require access to Fusion Framework® System™ components are required to sign an agreement and if needed, a Statement of Work ("SOW") for each project.	For a sample of new contractors that required access to Fusion Framework® System™ components, inquired of Fusion management and inspected the Independent Contractor Agreement to determine that it was signed.	No exceptions noted.

CC1.0: CONTROL ENVIRONMENT

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
CC1.3-05	For Fusion vendors that require their employees to have logical or physical access to Fusion Framework® System™ components, Fusion management assigns a Fusion employee to monitor and oversee the vendor employee's activities.	For a sample of new vendor employees that required logical or physical access to a Fusion Framework® System™ component, inquired of Fusion management and inspected the vendor MSA, SOW, or the vendor employee profile to determine that Fusion management assigned a Fusion employee to monitor and oversee the vendor employee's activities.	No exceptions noted.
CC1.4	<i>COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.</i>		
CC1.4-01	Fusion personnel are required to report any known violation of the Company's policies, including inappropriate business conduct, to their manager. Fusion managers are required to address any of these issues reported to them and notify HR as deemed necessary.	Inquired of Fusion management and inspected the performance improvement program report and correspondence from Fusion management to determine that Fusion personnel reported any known violation of the Company's policies, including inappropriate business conduct, to their manager, a Fusion manager addressed the only issues reported to them during the SOC 2® period, and HR was notified as deemed necessary.	No exceptions noted.
CC1.4-02	Fusion management interviews potential new personnel and contractors to determine if they have necessary skills and experience to meet job or project requirements.	For a sample of new personnel and new contractors, inquired of Fusion management and inspected the interview feedback forms to determine that Fusion management interviewed potential new personnel and contractors to determine if they had necessary skills and experience to meet job or project requirements.	No exceptions noted.

CC1.0: CONTROL ENVIRONMENT

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
CC1.4-03	Fusion policy requires background checks and drug testing for Fusion personnel and contractors to be initiated prior to employment or engagement start date.	For a sample of new personnel and new contractors, inquired of Fusion management and inspected the background check and drug test reports to determine that they were initiated prior to employment or engagement start date.	<u>New Personnel</u> Exception noted. For 1 of 10 new personnel selected for testing, that background check was initiated 1 week after start date. <u>New Contractors</u> No exceptions noted.
CC1.4-04	For vendor employees that require logical or physical access to Fusion Framework® System™ components, background check (or equivalent) is required.	For a sample of new vendor employees that required logical or physical access to a Fusion Framework® System™ component, inquired of Fusion management and inspected the background check or the requirement to obtain background check in the vendor agreement to determine that background checks were obtained.	No exceptions noted.
CC1.4-05	Fusion personnel are required to attend training ("New Hire Onboarding Series: Information Technology") within two weeks of hire date.	For a sample of new personnel, inquired of Fusion management and inspected the training logs from the learning management system or the training meeting invitations and agendas to determine that Fusion personnel attended the "New Hire Onboarding Series: Information Technology" training within two weeks of hire date.	No exceptions noted.
CC1.5	<i>COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.</i>		
CC1.5-01	Fusion senior management has established an organizational structure that includes authorities,	Inquired of Fusion management and inspected the current organization chart to determine that Fusion	No exceptions noted.

CC1.0: CONTROL ENVIRONMENT

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
	responsibilities and reporting lines relating to Fusion Framework® System™ security.	senior management established an organizational structure that included authorities, responsibilities and reporting lines relating to Fusion Framework® System™ security.	
CC1.5-02	Fusion senior management has assigned responsibility to implement, promulgate and monitor Fusion Framework® System™ controls to the Information Security Management Team.	Inquired of Fusion management and inspected the Information Security Management Team email distribution group and related job descriptions to determine that Fusion senior management assigned responsibility to implement, promulgate and monitor Fusion Framework® System™ controls to the Information Security Management Team.	No exceptions noted.
CC1.5-03	Fusion personnel (full-time employees, part-time employees, and interns) are required to acknowledge in writing within their first week of employment that they are responsible for reading and understanding the Fusion Employee Handbook.	For a sample of new personnel, inquired of Fusion management and inspected the Fusion Employee Handbook acknowledgement forms to determine that the Fusion Employee Handbook was acknowledged in writing within the first week of employment.	No exceptions noted.
CC1.5-04	Disciplinary action up to and including termination of employment is taken for violation of the Company's policies.	Inquired of Fusion management and inspected the performance improvement program report and correspondence from Fusion management to determine that disciplinary action up to and including termination of employment was taken for violation of the Company's policies.	No exceptions noted.

CC2.0: COMMUNICATION AND INFORMATION

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
CC2.1	<i>COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.</i>		
CC2.1-01	Fusion has implemented third-party tools to deliver the information needed to operate, maintain, and monitor the Fusion Framework® System™ and controls necessary to achieve customer commitments.	Inquired of Fusion management and inspected the third-party tool login pages or dashboards to determine that Fusion implemented third-party tools to deliver the information needed to operate, maintain, and monitor the Fusion Framework® System™ and controls necessary to achieve customer commitments.	No exceptions noted.
CC2.1-02	For Fusion Framework® System™ components located in the production environment at Salesforce, Fusion relies on Salesforce's vulnerability and network monitoring tools that are setup to send alerts to the responsible person or team at Fusion.	Inquired of Fusion management and inspected the Salesforce SOC 2® report and Fusion management's review of that report to determine that Fusion relied on Salesforce's vulnerability and network monitoring tools that were setup to send alerts to the responsible person or team at Fusion.	No exceptions noted.
CC2.1-03	As part of the risk management process, the Fusion Information Security Management Team considers whether additional tools or information resources are needed to meet Fusion Framework® System™ security objectives.	For a sample of weeks, inquired of Fusion management and inspected the current risk register and the minutes from the Fusion Information Security Management Team meetings with the vCISO to determine that as part of the risk management process, the Fusion Information Security Management Team considered whether additional tools or information resources were needed to meet Fusion Framework® System™ security objectives.	No exceptions noted.
CC2.1-04	As part of the risk management process, the Fusion Information Security Management Team considers if controls are adequate to mitigate identified risks and	For a sample of weeks, inquired of Fusion management and inspected the current risk register and the minutes from the Fusion Information Security Management Team	No exceptions noted.

CC2.0: COMMUNICATION AND INFORMATION

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
	meet control objectives, while developing and implementing changes if needed.	meetings with the vCISO to determine that as part of the risk management process, the Fusion Information Security Management Team considered if controls were adequate to mitigate identified risks and meet control objectives, while developing and implementing changes if needed.	
CC2.2	<i>COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.</i>		
CC2.2-01	Fusion designs and documents controls within the Fusion Policies and Procedures to mitigate risks according to the risk management strategy as defined by the Fusion Information Security Management Team.	Inquired of Fusion management and inspected the Fusion Policies and Procedures to determine that Fusion designed and documented controls within them.	No exceptions noted.
CC2.2-02	The Fusion Policies and Procedures are posted and available to Fusion personnel on the Company's intranet site.	Inquired of Fusion management and inspected links and user access to the Fusion Policies and Procedures on the Company's intranet site to determine that they were posted and available to Fusion personnel.	No exceptions noted.
CC2.2-03	Periodically, the Fusion Information Security Management Team assesses policies and procedures to ensure they remain appropriate to achieve business goals, including Fusion Framework® System™ security commitments. Changes to the policies and procedures require management approval.	Inquired of Fusion management and inspected the Fusion Policies and Procedures, and for a sample of weeks, inquired of Fusion management and inspected the current risk register and minutes from the Fusion Information Security Management Team meetings with the vCISO, to determine that the Fusion Information Security Management Team assessed policies and procedures periodically to ensure they remained	No exceptions noted.

CC2.0: COMMUNICATION AND INFORMATION

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
		appropriate to achieve business goals, including Fusion Framework® System™ security commitments, and changes were approved by Fusion management.	
CC2.2-04	Fusion personnel and contractors are required to attend security awareness training within two weeks of hire and annually thereafter.	For a sample of new personnel, new contractors, and existing personnel, inquired of Fusion management and inspected the learning management system logs or screen prints to determine that Fusion personnel and contractors attended security awareness training within two weeks of hire and annually thereafter.	<p><u>New Personnel</u> Exception noted. For 1 of 10 personnel selected for testing, security awareness training was attended about 4 weeks after hire date.</p> <p><u>New Contractors</u> No exceptions noted.</p> <p><u>Annual Training</u> No exceptions noted.</p>
CC2.2-05	For Fusion personnel, information regarding the Fusion Framework® System™ operation, boundaries and responsibilities is communicated as needed through the Fusion Policies and Procedures, Fusion Framework® System™ design documents, Fusion Framework® System™ release notes, and Salesforce platform training documentation.	Inquired of Fusion management and inspected the Fusion Policies and Procedures, Fusion Framework® System™ design documents, Fusion Framework® System™ release notes, and Salesforce platform training documentation to determine that they communicated information regarding the Fusion Framework® System™ operation, boundaries and responsibilities.	No exceptions noted.
CC2.2-06	For vendor employees that require logical or physical access to Fusion Framework® System™ components, information regarding the Fusion Framework® System™	For a sample of new vendor employees that required logical or physical access to a Fusion Framework® System™ component, inquired of Fusion management and inspected the vendor SOW or the project assignment	No exceptions noted.

CC2.0: COMMUNICATION AND INFORMATION

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
	is provided by Fusion management as deemed relevant to the services provided by the vendor.	form to determine that information regarding the Fusion Framework® System™ was provided by Fusion management as deemed relevant to the services provided by the vendor.	
CC2.2-07	For Fusion Framework® System™ components located in Chicago and Rolling Meadows, the Information Security Incident Management Policy and training presentation provide Fusion personnel and contractors with specific directions and responsibilities for reporting issues or incidents with the Fusion Framework® System™.	Inquired of Fusion management and inspected the Information Security Incident Management Policy and training presentations to determine that they provided Fusion personnel and contractors with specific directions and responsibilities for reporting issues or incidents with the Fusion Framework® System™.	No exceptions noted.
CC2.2-08	For Fusion Framework® System™ components located in the production environment at Salesforce, the Information Security Incident Management Policy provides Fusion personnel and contractors with specific directions and responsibilities for reporting issues or incidents with the Fusion Framework® System™.	Inquired of Fusion management and inspected the Information Security Incident Management Policy to determine that it provided Fusion personnel and contractors with specific directions and responsibilities for reporting issues or incidents with the Fusion Framework® System™.	No exceptions noted.
CC2.2-09	For changes to Fusion Framework® System™ components located in Chicago and Rolling Meadows, the Fusion Change Advisory Board ("CAB") considers security commitments and system requirements throughout the change process and notifies internal and external users as deemed necessary.	For a sample of change of Fusion Framework® System™ components located in Chicago and Rolling Meadows, inquired of Fusion management and inspected the help desk ticket and supporting documentation to determine that the Fusion CAB considered security commitments and system requirements throughout the change process and notified internal and external users as deemed necessary.	No exceptions noted.

CC2.0: COMMUNICATION AND INFORMATION

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
CC2.2-10	For global changes to the Fusion Framework® System™ components located in the production environment at Salesforce, the CAB considers security commitments and system requirements throughout the change process and notifies internal and external users as deemed necessary.	For a sample of global changes to the Fusion Framework® System™ components located in the production environment at Salesforce, inquired of Fusion management and inspected the help desk tickets and supporting documentation to determine that the CAB considered security commitments and system requirements throughout the change process and notified internal and external users as deemed necessary.	No exceptions noted.
CC2.2-11	For Fusion Framework® System™ existing customer post-implementation change requests, either a member of the Implementation Change Team or a member of Fusion's Delivery and Support Team consider security commitments and system requirements throughout the change process and notifies internal and external users as deemed necessary.	For a sample of customer post-implementation changes, inquired of Fusion management and inspected the statements of work to determine that a member of the Implementation Change Team or a member of Fusion's Delivery and Support Team considered security commitments and system requirements throughout the change process and notified internal and external users as deemed necessary.	No exceptions noted.
CC2.3	<i>COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.</i>		
CC2.3-01	For Fusion customers, information regarding the Fusion Framework® System™ is provided in the SOW as well as in the training documentation used to on-board new customers, and for on-going training and support.	For a sample of new customers, inquired of Fusion management and inspected the SOWs and the standard training presentations to determine that information regarding the Fusion Framework® System™ was provided to on-board new customers, and for on-going training and support.	No exceptions noted.

CC2.0: COMMUNICATION AND INFORMATION

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
CC2.3-02	Fusion's security commitments regarding the Fusion Framework® System™ are included in each customer's master services agreement ("MSA") and SOW. Fusion's legal counsel and the Director of Cyber Security review new customer MSAs that deviate from Fusion's standard MSA security-related language to ensure that Fusion is able to meet security commitments.	For a sample of new customers, inquired of Fusion management and inspected the MSAs and SOWs to determine that Fusion's security commitments regarding the Fusion Framework® System™ were included, and Fusion's legal counsel and the Director of Cyber Security reviewed new customer MSAs that deviated from Fusion's standard MSA security-related language to ensure that Fusion was able to meet security commitments.	No exceptions noted.
CC2.3-03	For global changes to the Fusion Framework® System™ components located in the production environment at Salesforce, the CAB considers security commitments and system requirements throughout the change process and notifies internal and external users as deemed necessary.	For a sample of global changes to the Fusion Framework® System™ components located in the production environment at Salesforce, inquired of Fusion management and inspected the help desk tickets and supporting documentation to determine that the CAB considered security commitments and system requirements throughout the change process and notified internal and external users as deemed necessary.	No exceptions noted.
CC2.3-04	For Fusion Framework® System™ existing customer post-implementation change requests, either a member of the Implementation Change Team or a member of Fusion's Delivery and Support Team consider security commitments and system requirements throughout the change process and notifies internal and external users as deemed necessary.	For a sample of customer post-implementation changes, inquired of Fusion management and inspected the statements of work to determine that a member of the Implementation Change Team or a member of Fusion's Delivery and Support Team considered security commitments and system requirements throughout the	No exceptions noted.

CC2.0: COMMUNICATION AND INFORMATION

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
		change process and notified internal and external users as deemed necessary.	
CC2.3-05	The "Complementary User Entity Controls" section of the Fusion SOC 2® report includes additional responsibilities for Fusion customers that are necessary to achieve certain control criteria.	Inquired of Fusion management and inspected the "Complementary User Entity Controls" section of the Fusion SOC 2® report to determine that it included additional responsibilities for Fusion customers that were necessary to achieve certain control criteria.	No exceptions noted.
CC2.3-06	Fusion customer responsibilities and procedures for reporting problems, system failures, or other issues related to security of the Fusion Framework® System™ are available on the Company's support portal.	Inquired of Fusion management and inspected an example case entry form on the Fusion customer portal and the case management dashboard to determine that Fusion customer responsibilities and procedures for reporting problems, system failures, or other issues related to security of the Fusion Framework® System™ are available on the Company's support portal.	No exceptions noted.

CC3.0: RISK ASSESSMENT

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
CC3.1	<i>COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.</i>		
CC3.1-01	Fusion senior management has established the Fusion Information Security Management Team to assist with	For a sample of weeks, inquired of Fusion management and inspected the current risk register and the minutes from the Fusion Information Security Management Team	No exceptions noted.

CC3.0: RISK ASSESSMENT

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
	the achievement of Fusion Framework® System™ security objectives.	meetings with the vCISO to determine that Fusion senior management established the Fusion Information Security Management Team to assist with the achievement of Fusion Framework® System™ security objectives.	
CC3.1-02	The Fusion Information Security Management Team has established a formal risk management process for managing Fusion Framework® System™ security risks.	For a sample of weeks, inquired of Fusion management and inspected the current risk register and the minutes from the Fusion Information Security Management Team meetings with the vCISO to determine that the Fusion Information Security Management Team established a formal risk management process for managing Fusion Framework® System™ security risks.	No exceptions noted.
CC3.1-03	As part of the risk management process, the Fusion Information Security Management Team assesses risk and assigns ratings based on factors such as likelihood and magnitude for the purpose of prioritizing risk treatment plans.	For a sample of weeks, inquired of Fusion management and inspected the current risk register and the minutes from the Fusion Information Security Management Team meetings with the vCISO to determine that as part of the risk management process, the Fusion Information Security Management Team assessed risk and assigned ratings based on factors such as likelihood and magnitude for the purpose of prioritizing risk treatment plans.	No exceptions noted.
CC3.1-04	Fusion's security commitments regarding the Fusion Framework® System™ are included in each customer's master services agreement ("MSA") and SOW. Fusion's legal counsel and the Director of Cyber Security review new customer MSAs that deviate from Fusion's standard	For a sample of new customers, inquired of Fusion management and inspected the MSAs and SOWs to determine that Fusion's security commitments regarding the Fusion Framework® System™ were included, and Fusion's legal counsel and the Director of Cyber Security	No exceptions noted.

CC3.0: RISK ASSESSMENT

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
	MSA security-related language to ensure that Fusion is able to meet security commitments.	reviewed new customer MSAs that deviated from Fusion's standard MSA security-related language to ensure that Fusion was able to meet security commitments.	
CC3.1-05	As part of the risk management process, the Fusion Information Security Management Team considers if controls are adequate to mitigate identified risks and meet control objectives, while developing and implementing changes if needed.	For a sample of weeks, inquired of Fusion management and inspected the current risk register and the minutes from the Fusion Information Security Management Team meetings with the vCISO to determine that as part of the risk management process, the Fusion Information Security Management Team considered if controls were adequate to mitigate identified risks and meet control objectives, while developing and implementing changes if needed.	No exceptions noted.
CC3.2	<i>COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.</i>		
CC3.2-01	The Fusion Information Security Management Team has established a formal risk management process for managing Fusion Framework® System™ security risks.	For a sample of weeks, inquired of Fusion management and inspected the current risk register and the minutes from the Fusion Information Security Management Team meetings with the vCISO to determine that the Fusion Information Security Management Team established a formal risk management process for managing Fusion Framework® System™ security risks.	No exceptions noted.
CC3.2-02	Annually for the Fusion Framework® System™ components located in Chicago and Rolling Meadows,	Inquired of Fusion management and inspected the most recent penetration testing reports, the remediation	No exceptions noted.

CC3.0: RISK ASSESSMENT

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
	the Company engages a third-party to perform penetration testing and Internal IT responds to issues identified.	maintenance process books, and minutes from the Fusion Information Security Management Team meetings with the vCISO to determine that penetration testing of the Fusion Framework® System™ components located in Chicago and Rolling Meadows was performed annually and Internal IT responded to issues identified.	
CC3.2-03	Annually for Fusion Framework® System™ components located in the production environment at Salesforce, the Company engages a third-party to perform penetration testing of the Fusion application and critical and high vulnerabilities, if any, are remediated as needed.	Inquired of Fusion management and inspected the most recent penetration testing summary letter, the remediation maintenance process books, and minutes from the Fusion Information Security Management Team meetings with the vCISO to determine that penetration testing of the Fusion application was performed annually and critical and high vulnerabilities were remediated as needed.	No exceptions noted.
CC3.2-04	For Fusion vendors that require their employees to have logical or physical access to Fusion Framework® System™ components, Fusion management assigns a Fusion employee to monitor and oversee the vendor employee's activities.	For a sample of new vendor employees that required logical or physical access to a Fusion Framework® System™ component, inquired of Fusion management and inspected the vendor MSA, SOW, or the vendor employee profile to determine that Fusion management assigned a Fusion employee to monitor and oversee the vendor employee's activities.	No exceptions noted.
CC3.2-05	At least monthly, the Fusion Information Security Management Team reviews results from network vulnerability scans (using third-party unified threat management software) and vulnerabilities identified by	For a sample of months, inquired of Fusion management and inspected the minutes from the Fusion Information Security Management Team meetings with the vCISO and the remediation maintenance process books to	No exceptions noted.

CC3.0: RISK ASSESSMENT

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
	the endpoint protection software and follows up on significant issues that are still open.	determine that at least monthly, the Fusion Information Security Management Team reviewed results from network vulnerability scans (using third-party unified threat management software) and followed up on significant issues that were still open.	
CC3.2-06	As part of the risk management process, the Fusion Information Security Management Team assesses risk and assigns ratings based on factors such as likelihood and magnitude for the purpose of prioritizing risk treatment plans.	For a sample of weeks, inquired of Fusion management and inspected the current risk register and the minutes from the Fusion Information Security Management Team meetings with the vCISO to determine that as part of the risk management process, the Fusion Information Security Management Team assessed risk and assigned ratings based on factors such as likelihood and magnitude for the purpose of prioritizing risk treatment plans.	No exceptions noted.
CC3.3	<i>COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.</i>		
CC3.3-01	As part of the risk management process, the Fusion Information Security Management Team considers fraud risk related to IT resources and customer data.	For a sample of weeks, inquired of Fusion management and inspected the current risk register and the minutes from the Fusion Information Security Management Team meetings with the vCISO to determine that as part of the risk management process, the Fusion Information Security Management Team considered fraud risk related to IT resources and customer data.	No exceptions noted.
CC3.3-02	Fusion has implemented third-party unified threat management and endpoint protection software (setup	For a sample of servers and laptops, inquired of Fusion management and inspected a report from, and the	No exceptions noted.

CC3.0: RISK ASSESSMENT

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
	with automatic updates) on servers located in Chicago and Rolling Meadows offices and laptops to monitor for suspicious activities.	dashboard of, the threat management and endpoint protection software, and the server configurations to determine that unified threat management and endpoint protection software was implemented and setup with automatic updates.	
CC3.3-03	For Fusion Framework® System™ components located in the production environment at Salesforce, Fusion relies on Salesforce's vulnerability and network monitoring tools that are setup to send alerts to the responsible person or team at Fusion.	Inquired of Fusion management and inspected the Salesforce SOC 2® report and Fusion management's review of that report to determine that Fusion relied on Salesforce's vulnerability and network monitoring tools that were setup to send alerts to the responsible person or team at Fusion.	No exceptions noted.
CC3.3-04	For Fusion Framework® System™ components located in Chicago and Rolling Meadows, hard drives on servers and laptops that reach the end of their useful life are fully wiped prior to disposition.	Inquired of Fusion management and inspected correspondence from Fusion management to determine that hard drives on servers and laptops that reached the end of their useful life were fully wiped prior to disposition.	FGMK was not able to test operating effectiveness of this control as there were no physical servers or laptops disposed during the SOC 2® period.
CC3.3-05	For Fusion customers that terminate services (request Fusion to cancel their license with Salesforce), Fusion notifies Salesforce to lock and delete the customer's Salesforce Org and related data according to Salesforce's standard procedures.	For a sample of terminated customers, inquired of Fusion management and inspected the cancelation orders and email correspondence between Fusion and Salesforce to determine that Salesforce locked and deleted the customer's Salesforce Org and related data according to Salesforce's standard procedures.	No exceptions noted.

CC3.0: RISK ASSESSMENT

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
CC3.3-06	Fusion relies on Salesforce to remove customer data from the Salesforce environment when the client terminates Fusion services.	Inquired of Fusion management and inspected the Salesforce SOC 2® report and Fusion management's review of that report to determine that Fusion relied on Salesforce to remove customer data from the Salesforce environment when the client terminated Fusion services.	No exceptions noted.
CC3.4	<i>COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.</i>		
CC3.4-01	The Fusion Information Security Management Team has established a formal risk management process for managing Fusion Framework® System™ security risks.	For a sample of weeks, inquired of Fusion management and inspected the current risk register and the minutes from the Fusion Information Security Management Team meetings with the vCISO to determine that the Fusion Information Security Management Team established a formal risk management process for managing Fusion Framework® System™ security risks.	No exceptions noted.
CC3.4-02	As part of the risk management process, the Fusion Information Security Management Team assesses risk and assigns ratings based on factors such as likelihood and magnitude for the purpose of prioritizing risk treatment plans.	For a sample of weeks, inquired of Fusion management and inspected the current risk register and the minutes from the Fusion Information Security Management Team meetings with the vCISO to determine that as part of the risk management process, the Fusion Information Security Management Team assessed risk and assigned ratings based on factors such as likelihood and magnitude for the purpose of prioritizing risk treatment plans.	No exceptions noted.

CC4.0: MONITORING ACTIVITIES

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
CC4.1	<i>COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.</i>		
CC4.1-01	The Fusion Information Security Management Team has established a formal risk management process for managing Fusion Framework® System™ security risks.	For a sample of weeks, inquired of Fusion management and inspected the current risk register and the minutes from the Fusion Information Security Management Team meetings with the vCISO to determine that the Fusion Information Security Management Team established a formal risk management process for managing Fusion Framework® System™ security risks.	No exceptions noted.
CC4.1-02	As part of the risk management process, the Fusion Information Security Management Team assesses risk and assigns ratings based on factors such as likelihood and magnitude for the purpose of prioritizing risk treatment plans.	For a sample of weeks, inquired of Fusion management and inspected the current risk register and the minutes from the Fusion Information Security Management Team meetings with the vCISO to determine that as part of the risk management process, the Fusion Information Security Management Team assessed risk and assigned ratings based on factors such as likelihood and magnitude for the purpose of prioritizing risk treatment plans.	No exceptions noted.
CC4.1-03	Annually for Fusion Framework® System™ components located in the production environment at Salesforce, the Company engages a third-party to perform penetration testing of the Fusion application and critical and high vulnerabilities, if any, are remediated as needed.	Inquired of Fusion management and inspected the most recent penetration testing summary letter, the remediation maintenance process books, and minutes from the Fusion Information Security Management Team meetings with the vCISO to determine that penetration testing of the Fusion application was performed annually	No exceptions noted.

CC4.0: MONITORING ACTIVITIES

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
		and critical and high vulnerabilities were remediated as needed.	
CC4.1-04	Fusion has implemented third-party unified threat management and endpoint protection software (setup with automatic updates) on servers located in Chicago and Rolling Meadows offices and laptops to monitor for suspicious activities.	For a sample of servers and laptops, inquired of Fusion management and inspected a report from, and the dashboard of, the threat management and endpoint protection software, and the server configurations to determine that unified threat management and endpoint protection software was implemented and setup with automatic updates.	No exceptions noted.
CC4.1-05	For Fusion Framework® System™ components located in the production environment at Salesforce, Fusion relies on Salesforce's vulnerability and network monitoring tools that are setup to send alerts to the responsible person or team at Fusion.	Inquired of Fusion management and inspected the Salesforce SOC 2® report and Fusion management's review of that report to determine that Fusion relied on Salesforce's vulnerability and network monitoring tools that were setup to send alerts to the responsible person or team at Fusion.	No exceptions noted.
CC4.2	<i>COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.</i>		
CC4.2-01	The Fusion Information Security Management Team has established a formal risk management process for managing Fusion Framework® System™ security risks.	For a sample of weeks, inquired of Fusion management and inspected the current risk register and the minutes from the Fusion Information Security Management Team meetings with the vCISO to determine that the Fusion Information Security Management Team established a formal risk management process for managing Fusion Framework® System™ security risks.	No exceptions noted.

CC4.0: MONITORING ACTIVITIES

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
CC4.2-02	As part of the risk management process, the Fusion Information Security Management Team assesses risk and assigns ratings based on factors such as likelihood and magnitude for the purpose of prioritizing risk treatment plans.	For a sample of weeks, inquired of Fusion management and inspected the current risk register and the minutes from the Fusion Information Security Management Team meetings with the vCISO to determine that as part of the risk management process, the Fusion Information Security Management Team assessed risk and assigned ratings based on factors such as likelihood and magnitude for the purpose of prioritizing risk treatment plans.	No exceptions noted.
CC4.2-03	Fusion control owners and members of the Fusion Information Security Management Team are required to report actual or potential control deficiencies, if any, to the Director of Cyber Security.	Inquired of Fusion management and inspected the controls matrix and correspondence from Fusion management to determine that Fusion control owners and members of the Fusion Information Security Management Team were required to report actual or potential control deficiencies to the Director of Cyber Security, and there were no actual or potential control deficiencies during the SOC 2® period.	No exceptions noted.

CC5.0: CONTROL ACTIVITIES

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
CC5.1	<i>COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.</i>		
CC5.1-01	The Fusion Information Security Management Team has established a formal risk management process for managing Fusion Framework® System™ security risks.	For a sample of weeks, inquired of Fusion management and inspected the current risk register and the minutes from the Fusion Information Security Management Team meetings with the vCISO to determine that the Fusion Information Security Management Team established a formal risk management process for managing Fusion Framework® System™ security risks.	No exceptions noted.
CC5.1-02	As part of the risk management process, the Fusion Information Security Management Team assesses risk and assigns ratings based on factors such as likelihood and magnitude for the purpose of prioritizing risk treatment plans.	For a sample of weeks, inquired of Fusion management and inspected the current risk register and the minutes from the Fusion Information Security Management Team meetings with the vCISO to determine that as part of the risk management process, the Fusion Information Security Management Team assessed risk and assigned ratings based on factors such as likelihood and magnitude for the purpose of prioritizing risk treatment plans.	No exceptions noted.
CC5.1-03	As part of the risk management process, the Fusion Information Security Management Team considers if controls are adequate to mitigate identified risks and meet control objectives, while developing and implementing changes if needed.	For a sample of weeks, inquired of Fusion management and inspected the current risk register and the minutes from the Fusion Information Security Management Team meetings with the vCISO to determine that as part of the risk management process, the Fusion Information Security Management Team considered if controls were adequate to mitigate identified risks and meet control	No exceptions noted.

CC5.0: CONTROL ACTIVITIES

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
		objectives, while developing and implementing changes if needed.	
CC5.1-04	Fusion designs and documents controls within the Fusion Policies and Procedures to mitigate risks according to the risk management strategy as defined by the Fusion Information Security Management Team.	Inquired of Fusion management and inspected the Fusion Policies and Procedures to determine that Fusion designed and documented controls within them.	No exceptions noted.
CC5.1-05	The Fusion Policies and Procedures are posted and available to Fusion personnel on the Company's intranet site.	Inquired of Fusion management and inspected links and user access to the Fusion Policies and Procedures on the Company's intranet site to determine that they were posted and available to Fusion personnel.	No exceptions noted.
CC5.2	<i>COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.</i>		
CC5.2-01	The Fusion Information Security Management Team has considered general controls over technology throughout this controls matrix to achieve Fusion Framework® System™ security objectives.	Inquired of Fusion management and inspected the controls matrix to determine that the Fusion Information Security Management Team considered general controls over technology throughout it to achieve Fusion Framework® System™ security objectives.	No exceptions noted.
CC5.3	<i>COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.</i>		
CC5.3-01	As part of the risk management process, the Fusion Information Security Management Team considers if controls are adequate to mitigate identified risks and	For a sample of weeks, inquired of Fusion management and inspected the current risk register and the minutes from the Fusion Information Security Management Team meetings with the vCISO to determine that as part of the	No exceptions noted.

CC5.0: CONTROL ACTIVITIES

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
	meet control objectives, while developing and implementing changes if needed.	risk management process, the Fusion Information Security Management Team considered if controls were adequate to mitigate identified risks and meet control objectives, while developing and implementing changes if needed.	
CC5.3-02	Fusion designs and documents controls within the Fusion Policies and Procedures to mitigate risks according to the risk management strategy as defined by the Fusion Information Security Management Team.	Inquired of Fusion management and inspected the Fusion Policies and Procedures to determine that Fusion designed and documented controls within them.	No exceptions noted.
CC5.3-03	The Fusion Policies and Procedures are posted and available to Fusion personnel on the Company's intranet site.	Inquired of Fusion management and inspected links and user access to the Fusion Policies and Procedures on the Company's intranet site to determine that they were posted and available to Fusion personnel.	No exceptions noted.
CC5.3-04	Periodically, the Fusion Information Security Management Team assesses policies and procedures to ensure they remain appropriate to achieve business goals, including Fusion Framework® System™ security commitments. Changes to the policies and procedures require management approval.	Inquired of Fusion management and inspected the Fusion Policies and Procedures, and for a sample of weeks, inquired of Fusion management and inspected the current risk register and minutes from the Fusion Information Security Management Team meetings with the vCISO, to determine that the Fusion Information Security Management Team assessed policies and procedures periodically to ensure they remained appropriate to achieve business goals, including Fusion Framework® System™ security commitments, and changes were approved by Fusion management.	No exceptions noted.

CC6.0: LOGICAL AND PHYSICAL ACCESS CONTROLS

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
CC6.1	<i>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.</i>		
CC6.1-01	The Company maintains an asset inventory and each asset is assigned an owner that is responsible for physical and logical access, including each Salesforce Org.	Inquired of Fusion management and inspected the asset inventory spreadsheets to determine that they were maintained and each asset was assigned an owner that was responsible for physical and logical access, including each Salesforce Org.	No exceptions noted.
CC6.1-02	For Fusion Framework® System™ components located in Chicago and Rolling Meadows, logical access is controlled through either MS Active Directory integration when possible or through each component's native security.	For a sample of months, inquired of Fusion management and inspected the help desk tickets of Fusion management's monthly review of logical user access to determine that logical access was controlled through either MS Active Directory integration when possible or through each component's native security.	No exceptions noted.
CC6.1-03	For Fusion Framework® System™ components located in the production environment at Salesforce, logical access for Fusion personnel is managed through its third-party identity management solution, Okta.	Inquired of Fusion management and inspected the single sign-on configuration of Fusion's production environment at Salesforce to determine that logical access for Fusion personnel was managed through its third-party identity management solution, Okta.	No exceptions noted.
CC6.1-04	For Fusion Framework® System™ components located in Chicago and Rolling Meadows, Fusion personnel gain remote access to the Fusion Framework® System™ using a third-party VPN solution which requires a valid MS	Inquired of Fusion management and observed a logon attempt from a remote workstation to determine that VPN required a valid MS Active Directory user ID and password that had been added to the MS Active Directory VPN users groups.	No exceptions noted.

CC6.0: LOGICAL AND PHYSICAL ACCESS CONTROLS

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
	Active Directory user ID and password that has been added to the MS Active Directory VPN users groups.		
CC6.1-05	For Fusion Framework® System™ components located in Chicago and Rolling Meadows, system or generic administrative accounts are only used as required with passwords known to the Internal IT Team.	For a sample of months, inquired of Fusion management and inspected the help desk tickets of Fusion management's monthly review of logical user access to determine that system or generic administrative accounts were only used as required with passwords known to the Internal IT Team.	No exceptions noted.
CC6.1-06	<p>MS Active Directory and JAMF, which control access to the Chicago and Rolling Meadows local network, are setup to follow documented Company policy that includes:</p> <p>1) force password change after a defined number of days; 2) require passwords to follow defined complexity rules; and 3) lock user ID after a defined number of unsuccessful login attempts.</p>	<p>Inquired of Fusion management and inspected the MS Active Directory and JAMF password configurations to determine that MS Active Directory and JAMF were setup to follow documented Company policy that included:</p> <p>1) force password change after a defined number of days; 2) require passwords to follow defined complexity rules; and 3) lock user ID after a defined number of unsuccessful login attempts.</p>	No exceptions noted.
CC6.1-07	<p>Okta, which controls Fusion personnel access to the Fusion Framework® System™ components located in the production environment at Salesforce, is setup to follow documented Company policy that includes:</p> <p>1) force password change after a defined number of</p>	<p>Inquired of Fusion management and inspected the Okta password and multi-factor authentication configurations to determine that Okta was setup to follow documented Company policy that included:</p> <p>1) force password change after a defined number of</p>	No exceptions noted.

CC6.0: LOGICAL AND PHYSICAL ACCESS CONTROLS

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
	days; 2) require passwords to follow defined complexity rules; 3) lock user ID after a defined number of unsuccessful login attempts; and 4) multi-factor authentication.	days; 2) require passwords to follow defined complexity rules; 3) lock user ID after a defined number of unsuccessful login attempts; and 4) multi-factor authentication.	
CC6.2	<i>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.</i>		
CC6.2-01	Logical access to Fusion Framework® System™ components in Chicago and Rolling Meadows requires approval by HR or an authorized Fusion manager.	For a sample of new personnel, new contractors, and new vendor employees, inquired of Fusion management and inspected the help desk tickets to determine that logical access to Fusion Framework® System™ components in Chicago and Rolling Meadows was approved by HR or an authorized Fusion manager.	No exceptions noted.
CC6.2-02	Logical access to Fusion Framework® System™ components in Salesforce.com requires approval by HR or an authorized Fusion manager.	For a sample of new personnel, new contractors, and new vendor employees, inquired of Fusion management and inspected the help desk tickets to determine that logical access to Fusion Framework® System™ components in Salesforce.com was approved by HR or an authorized Fusion manager.	No exceptions noted.
CC6.2-03	Monthly, the Directory of Security reviews Okta user accounts (including administrator accounts) to ensure access is limited to authorized Fusion users as needed.	For a sample of months, inquired of Fusion management and inspected the help desk tickets to determine that the Directory of Security reviewed Okta user accounts	Exceptions noted. For 4 of 4 months selected for testing, the help desk tickets indicated that user accounts were compared to the HR listing of active

CC6.0: LOGICAL AND PHYSICAL ACCESS CONTROLS

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
		(including administrator accounts) to ensure access was limited to authorized Fusion users as needed.	Fusion personnel, however, review of Okta administrator access was not documented.
CC6.2-04	Logical access to Fusion Framework® System™ components is removed within the timeframe as requested by Fusion management.	For a sample of separations, inquired of Fusion management and inspected the help desk tickets to determine that logical access to Fusion Framework® System™ components was removed within the timeframe as requested by Fusion management.	No exceptions noted.
CC6.2-05	Monthly, Fusion management reviews MS Active Directory user accounts (including system or generic administrative accounts) to ensure access is limited to authorized Fusion users as needed.	For a sample of months, inquired of Fusion management and inspected the help desk tickets to determine that monthly, Fusion management reviewed MS Active Directory user accounts (including system or generic administrative accounts) to ensure access was limited to authorized Fusion users as needed.	No exceptions noted.
CC6.3	<i>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.</i>		
CC6.3-01	Logical access to Fusion Framework® System™ components in Chicago and Rolling Meadows requires approval by HR or an authorized Fusion manager.	For a sample of new personnel, new contractors, and new vendor employees, inquired of Fusion management and inspected the help desk tickets to determine that logical access to Fusion Framework® System™ components in Chicago and Rolling Meadows was approved by HR or an authorized Fusion manager.	No exceptions noted.

CC6.0: LOGICAL AND PHYSICAL ACCESS CONTROLS

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
CC6.3-02	Logical access to Fusion Framework® System™ components in Salesforce.com requires approval by HR or an authorized Fusion manager.	For a sample of new personnel, new contractors, and new vendor employees, inquired of Fusion management and inspected the help desk tickets to determine that logical access to Fusion Framework® System™ components in Salesforce.com was approved by HR or an authorized Fusion manager.	No exceptions noted.
CC6.3-03	Monthly, the Directory of Security reviews Okta user accounts (including administrator accounts) to ensure access is limited to authorized Fusion users as needed.	For a sample of months, inquired of Fusion management and inspected the help desk tickets to determine that the Directory of Security reviewed Okta user accounts (including administrator accounts) to ensure access was limited to authorized Fusion users as needed.	Exceptions noted. For 4 of 4 months selected for testing, the help desk tickets indicated that user accounts were compared to the HR listing of active Fusion personnel, however, review of Okta administrator access was not documented.
CC6.3-04	For Fusion Framework® System™ components located in Chicago and Rolling Meadows, logical access is controlled through either MS Active Directory integration when possible or through each component's native security.	For a sample of months, inquired of Fusion management and inspected the help desk tickets of Fusion management's monthly review of logical user access to determine that logical access was controlled through either MS Active Directory integration when possible or through each component's native security.	No exceptions noted.
CC6.3-05	For Fusion Framework® System™ components located in the production environment at Salesforce, logical access for Fusion personnel is managed through its third-party identity management solution, Okta.	Inquired of Fusion management and inspected the single sign-on configuration of Fusion's production environment at Salesforce to determine that logical access for Fusion personnel was managed through its third-party identity management solution, Okta.	No exceptions noted.

CC6.0: LOGICAL AND PHYSICAL ACCESS CONTROLS

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
CC6.3-06	Monthly, Fusion management reviews MS Active Directory user accounts (including system or generic administrative accounts) to ensure access is limited to authorized Fusion users as needed.	For a sample of months, inquired of Fusion management and inspected the help desk tickets to determine that monthly, Fusion management reviewed MS Active Directory user accounts (including system or generic administrative accounts) to ensure access was limited to authorized Fusion users as needed.	No exceptions noted.
CC6.3-07	Logical access to Fusion Framework® System™ components is removed within the timeframe as requested by Fusion management.	For a sample of separations, inquired of Fusion management and inspected the help desk tickets to determine that logical access to Fusion Framework® System™ components is removed within the timeframe as requested by Fusion management.	No exceptions noted.
CC6.4	<i>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.</i>		
CC6.4-01	<p>Rolling Meadows The office suite is protected by a key card system, and the emergency exit door and server cage are protected by physical lock and key.</p> <p>Chicago The office suite and server room are protected by a key card system.</p> <p>London</p>	Inquired of Fusion management and inspected, inspected current pictures of (and observed during a prior year's SOC 2® examination) the office suites in Chicago and Rolling Meadows, and inspected current videos of the London office to determine that for Rolling Meadows, the office suite was protected by a key card system, and the emergency exit door and server cage were protected by physical lock and key, for Chicago, the office suite and server room were protected by a key card system, and for London, the offices within the shared workspace were protected by a key card system.	No exceptions noted.

CC6.0: LOGICAL AND PHYSICAL ACCESS CONTROLS

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
	The offices within the shared workspace are protected by a key card system.		
CC6.4-02	Physical access to Fusion's offices, server rooms, or server cage requires approval by HR or an authorized Fusion manager.	For a sample of new personnel, new contractors, and new vendor employees, inquired of Fusion management and inspected the help desk tickets to determine that physical access to Fusion's offices, server rooms, or server cage was approved by HR or an authorized Fusion manager.	No exceptions noted.
CC6.4-03	Visitors to Fusion offices are required to be escorted to the person that they are visiting.	Inquired of Fusion management, inspected correspondence from Fusion management, inspected current pictures of (and observed during a prior year's SOC 2® examination) the office suites in Chicago and Rolling Meadows, and inspected current videos of the London office to determine that visitors to Fusion offices were required to be escorted to the person that they were visiting.	No exceptions noted.
CC6.4-04	Physical access to the Fusion office suites, server room, and server cage is removed within the timeframe as requested by Fusion management.	For a sample of separations, inquired of Fusion management and inspected the help desk tickets to determine that physical access to the Fusion office suites, server room, and server cage was removed within the timeframe as requested by Fusion management.	Exceptions noted. For 3 of 5 separations, physical access was revoked 3 days, 6 days, and 22 days after the separation and request date.
CC6.4-05	Monthly for Fusion offices in Chicago and Rolling Meadows, Fusion management reviews active key cards and physical key distribution to ensure that physical	For a sample of months, inquired of Fusion management and inspected the help desk tickets and supporting documentation to determine that Fusion management	No exceptions noted.

CC6.0: LOGICAL AND PHYSICAL ACCESS CONTROLS

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
	access to the office suites, server room, and server cage remains authorized.	reviewed active key cards and physical key distribution to ensure that physical access to the Fusion Chicago and Rolling Meadows office suites, server room, and server cage remained authorized.	
CC6.4-06	Monthly for the Rolling Meadows office, temporary key cards are inventoried and if any are missing, the key card is deactivated. The Fusion Chicago office does not have temporary key cards for the office suite.	For a sample of months, inquired of Fusion management and inspected the help desk tickets and supporting documentation to determine that temporary key cards for the Rolling Meadows office were inventoried and missing key cards, if any, were deactivated.	No exceptions noted.
CC6.4-07	Monthly for shared workspace in London, Fusion management reviews a list of users with physical access to ensure that physical access to the office suite remains authorized.	For a sample of months, inquired of Fusion management and inspected email correspondence with screen prints from the physical access system to determine that Fusion management reviewed a list of users with physical access to the shared workspace in London to ensure that physical access remained authorized.	No exceptions noted.
CC6.5	<i>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.</i>		
CC6.5-01	For Fusion customers that terminate services (request Fusion to cancel their license with Salesforce), Fusion notifies Salesforce to lock and delete the customer's Salesforce Org and related data according to Salesforce's standard procedures.	For a sample of terminated customers, inquired of Fusion management and inspected the cancelation orders and email correspondence between Fusion and Salesforce to determine that Salesforce locked and deleted the customer's Salesforce Org and related data according to Salesforce's standard procedures.	No exceptions noted.

CC6.0: LOGICAL AND PHYSICAL ACCESS CONTROLS

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
CC6.5-02	Fusion relies on Salesforce to remove customer data from the Salesforce environment when the client terminates Fusion services.	Inquired of Fusion management and inspected the Salesforce SOC 2® report and Fusion management's review of that report to determine that Fusion relied on Salesforce to remove customer data from the Salesforce environment when the client terminated Fusion services.	No exceptions noted.
CC6.5-03	For Fusion Framework® System™ components located in Chicago and Rolling Meadows, hard drives on servers and laptops that reach the end of their useful life are fully wiped prior to disposition.	Inquired of Fusion management and inspected correspondence from Fusion management to determine that hard drives on servers and laptops that reached the end of their useful life were fully wiped prior to disposition.	FGMK was not able to test operating effectiveness of this control as there were no physical servers or laptops disposed during the SOC 2® period.
CC6.6	<i>The entity implements logical access security measures to protect against threats from sources outside its system boundaries.</i>		
CC6.6-01	Annually for Chicago and Rolling Meadows, Fusion engages a third-party to review and update the firewall rules and configuration.	Inquired of Fusion management and inspected the project description in the invoice to determine that Fusion engaged a third-party annually to review and update the firewall rules and configuration.	No exceptions noted.
CC6.6-02	For Fusion Framework® System™ components located in Chicago and Rolling Meadows, Fusion personnel gain remote access to the Fusion Framework® System™ using a third-party VPN solution which requires a valid MS Active Directory user ID and password that has been added to the MS Active Directory VPN users groups.	Inquired of Fusion management and observed a logon attempt from a remote workstation to determine that VPN required a valid MS Active Directory user ID and password that had been added to the MS Active Directory VPN users groups.	No exceptions noted.
CC6.6-03	Logical access to Fusion Framework® System™ components located in the production environment at	Inquired of Fusion management and inspected Fusion's Salesforce home page settings to determine that logical	No exceptions noted.

CC6.0: LOGICAL AND PHYSICAL ACCESS CONTROLS

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
	Salesforce is over an encrypted Transport Layer Security ("TLS") session.	access to Fusion Framework® System™ components located in the production environment at Salesforce was over an encrypted TLS session.	
CC6.6-04	Fusion uses cloud-based email which is setup to scan inbound and outbound email according to the vendor's default policy, which includes scanning for potentially malicious attachments and other email content.	Inquired of Fusion management and inspected the cloud-based email dashboard and scanning configurations to determine that cloud-based email was setup to scan inbound and outbound email according to the vendor's default policy, which included scanning for potentially malicious attachments and other email content.	No exceptions noted.
CC6.6-05	Annually for Fusion Framework® System™ components located in the production environment at Salesforce, the Company engages a third-party to perform penetration testing of the Fusion application and critical and high vulnerabilities, if any, are remediated as needed.	Inquired of Fusion management and inspected the most recent penetration testing summary letter, the remediation maintenance process books, and minutes from the Fusion Information Security Management Team meetings with the vCISO to determine that penetration testing of the Fusion application was performed annually and critical and high vulnerabilities were remediated as needed.	No exceptions noted.
CC6.6-06	At least monthly, the Fusion Information Security Management Team reviews results from network vulnerability scans (using third-party unified threat management software) and vulnerabilities identified by the endpoint protection software and follows up on significant issues that are still open.	For a sample of months, inquired of Fusion management and inspected the minutes from the Fusion Information Security Management Team meetings with the vCISO and the remediation maintenance process books to determine that at least monthly, the Fusion Information Security Management Team reviewed results from network vulnerability scans (using third-party unified	No exceptions noted.

CC6.0: LOGICAL AND PHYSICAL ACCESS CONTROLS

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
		threat management software) and followed up on significant issues that were still open.	
CC6.6-07	Fusion has implemented third-party unified threat management and endpoint protection software (setup with automatic updates) on servers located in Chicago and Rolling Meadows offices and laptops to monitor for suspicious activities.	For a sample of servers and laptops, inquired of Fusion management and inspected a report from, and the dashboard of, the threat management and endpoint protection software, and the server configurations to determine that unified threat management and endpoint protection software was implemented and setup with automatic updates.	No exceptions noted.
CC6.6-08	For Fusion Framework® System™ components located in the production environment at Salesforce, Fusion relies on Salesforce's vulnerability and network monitoring tools that are setup to send alerts to the responsible person or team at Fusion.	Inquired of Fusion management and inspected the Salesforce SOC 2® report and Fusion management's review of that report to determine that Fusion relied on Salesforce's vulnerability and network monitoring tools that were setup to send alerts to the responsible person or team at Fusion.	No exceptions noted.
CC6.7	<i>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.</i>		
CC6.7-01	Laptop hard drives are encrypted (BitLocker for PC's and Sophos Endpoint Device Encryption for Mac's).	For a sample of laptops, inquired of Fusion management and inspected a report from, or the device configuration screen prints from, the threat management and endpoint protection software to determine that hard drives were encrypted.	No exceptions noted.

CC6.0: LOGICAL AND PHYSICAL ACCESS CONTROLS

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
CC6.7-02	Fusion's third-party cloud document storage site is encrypted.	Inquired of Fusion management and inspected the third-party's public posting of its description of its security and encryption of its cloud storage environment to determine that it was encrypted.	No exceptions noted.
CC6.7-03	For Fusion Framework® System™ components located in the production environment at Salesforce, Fusion relies on Salesforce's data backup and encryption policies and controls.	Inquired of Fusion management and inspected the Salesforce SOC 2® report and Fusion management's review of that report to determine that Fusion relied on Salesforce's data backup and encryption policies and controls.	No exceptions noted.
CC6.7-04	Company policy prohibits storing customer data in non-approved cloud storage.	Inquired of Fusion management and inspected the Fusion Acceptable Use Policy and the firewall configurations to determine that Company policy prohibited storing customer data in non-approved cloud storage.	No exceptions noted.
CC6.8	<i>The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.</i>		
CC6.8-01	The ability to install software or make configuration changes to servers and firewalls in Chicago and RMO offices, and laptops is restricted to authorized Fusion IT personnel.	For a sample of servers and laptops, inquired of Fusion management and inspected local administrator access configurations to determine that the ability to install software or make configuration changes to servers and firewalls in Chicago and RMO offices, and laptops was restricted to authorized Fusion IT personnel.	<u>Servers and Firewalls</u> No exceptions noted. <u>Laptops</u> Exceptions noted. For 2 of 41 laptops selected for testing, temporary administrator accounts (1 on each laptop, with ability to install software or make

CC6.0: LOGICAL AND PHYSICAL ACCESS CONTROLS

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
			<p>configuration changes) were present. FGMK inquired of Fusion management to determine that they were authorized, and they were setup for specific, short-term needs. However, the approvals of that temporary administrator access were not available.</p> <p>Subsequent to FGMK's testing, Fusion removed these 2 accounts on these 2 laptops and FGMK inspected screen prints to determine that they were removed.</p>
CC6.8-02	Weekly, members of the Fusion Information Security Management Team review the vulnerability management application dashboard and determines if patches to servers located in Chicago and Rolling Meadows offices and laptops are deemed necessary.	For a sample of weeks, inquired of Fusion management and inspected the vulnerability trackers, the minutes from the Fusion Information Security Management Team meetings with the vCISO, and the remediation maintenance process books to determine that members of the Fusion Information Security Management Team reviewed the vulnerability management application dashboard and determined if patches to servers located in Chicago and Rolling Meadows offices and laptops were deemed necessary.	No exceptions noted.
CC6.8-03	Fusion has implemented third-party unified threat management and endpoint protection software (setup with automatic updates) on servers located in Chicago	For a sample of servers and laptops, inquired of Fusion management and inspected a report from, and the dashboard of, the threat management and endpoint	No exceptions noted.

CC6.0: LOGICAL AND PHYSICAL ACCESS CONTROLS

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
	and Rolling Meadows offices and laptops to monitor for suspicious activities.	protection software, and the server configurations to determine that unified threat management and endpoint protection software was implemented and setup with automatic updates.	
CC6.8-04	The endpoint protection software on Fusion servers located in Chicago and Rolling Meadows offices and laptops can only be disabled or removed by an administrator with endpoint software management console access.	Inquired of Fusion management and inspected a screen print of the tamper protection configuration to determine that the endpoint protection software on Fusion servers located in Chicago and Rolling Meadows offices and laptops could only be disabled or removed by an administrator with endpoint software management console access.	No exceptions noted.
CC6.8-05	Access to the endpoint software management console is restricted to a limited number of authorized Fusion personnel.	Inquired of Fusion management and inspected the endpoint software user listing and Fusion management's review to determine that access to the endpoint software management console was restricted to a limited number of authorized Fusion personnel.	No exceptions noted.
CC6.8-06	The endpoint protection software on Fusion servers located in Chicago and Rolling Meadows offices and laptops is configured to send automated alerts to the Internal IT Team and the Fusion Information Security Management Team if potentially malicious software is identified on Fusion servers or laptops.	Inquired of Fusion management and inspected the global configuration of the endpoint software to determine that it was configured to send automated alerts to the Internal IT Team and the Fusion Information Security Management Team if potentially malicious software was identified on Fusion servers or laptops.	No exceptions noted.
CC6.8-07	Weekly, For Fusion Framework® System™ components located in Chicago and Rolling Meadows, a member of	For a sample of weeks, inquired of Fusion management and inspected the help desk tickets and the endpoint	No exceptions noted.

CC6.0: LOGICAL AND PHYSICAL ACCESS CONTROLS

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
	the Internal IT Team investigates and resolves issues relating to alerts from the endpoint protection software which were not automatically quarantined.	protection software dashboard screen prints to determine that a member of the Internal IT Team investigated and resolved issues relating to alerts from the endpoint protection software which were not automatically quarantined.	
CC6.8-08	Fusion has implemented third-party unified threat management and endpoint protection software (setup with automatic updates) on servers located in Chicago and Rolling Meadows offices and laptops to monitor for suspicious activities.	For a sample of servers and laptops, inquired of Fusion management and inspected a report from, and the dashboard of, the threat management and endpoint protection software, and the server configurations to determine that unified threat management and endpoint protection software was implemented and setup with automatic updates.	No exceptions noted.
CC6.8-09	For Fusion Framework® System™ components located in the production environment at Salesforce, Fusion relies on Salesforce's vulnerability and network monitoring tools that are setup to send alerts to the responsible person or team at Fusion.	Inquired of Fusion management and inspected the Salesforce SOC 2® report and Fusion management's review of that report to determine that Fusion relied on Salesforce's vulnerability and network monitoring tools that were setup to send alerts to the responsible person or team at Fusion.	No exceptions noted.
CC6.8-10	For Fusion Framework® System™ components located in the production environment at Salesforce, Fusion relies on Salesforce's antivirus and antimalware policies and controls.	Inquired of Fusion management and inspected the Salesforce SOC 2® report and Fusion management's review of that report to determine that Fusion relied on Salesforce's antivirus and antimalware policies and controls.	No exceptions noted.

CC7.0: SYSTEM OPERATIONS

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
CC7.1	<i>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.</i>		
CC7.1-01	Fusion has implemented third-party unified threat management and endpoint protection software (setup with automatic updates) on servers located in Chicago and Rolling Meadows offices and laptops to monitor for suspicious activities.	For a sample of servers and laptops, inquired of Fusion management and inspected a report from, and the dashboard of, the threat management and endpoint protection software, and the server configurations to determine that unified threat management and endpoint protection software was implemented and setup with automatic updates.	No exceptions noted.
CC7.1-02	For Fusion Framework® System™ components located in the production environment at Salesforce, Fusion relies on Salesforce's vulnerability and network monitoring tools that are setup to send alerts to the responsible person or team at Fusion.	Inquired of Fusion management and inspected the Salesforce SOC 2® report and Fusion management's review of that report to determine that Fusion relied on Salesforce's vulnerability and network monitoring tools that were setup to send alerts to the responsible person or team at Fusion.	No exceptions noted.
CC7.1-03	Annually for Fusion Framework® System™ components located in the production environment at Salesforce, the Company engages a third-party to perform penetration testing of the Fusion application and critical and high vulnerabilities, if any, are remediated as needed.	Inquired of Fusion management and inspected the most recent penetration testing summary letter, the remediation maintenance process books, and minutes from the Fusion Information Security Management Team meetings with the vCISO to determine that penetration testing of the Fusion application was performed annually and critical and high vulnerabilities were remediated as needed.	No exceptions noted.

CC7.0: SYSTEM OPERATIONS

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
CC7.1-04	Fusion Framework® System™ domain controllers located in Chicago and Rolling Meadows offices are configured to be backed up daily to a NAS in the Chicago office.	Inquired of Fusion management and inspected the backup software configurations to determine that fusion Framework® System™ domain controllers located in Chicago and Rolling Meadows offices were configured to be backed up daily to a NAS in the Chicago office.	No exceptions noted.
CC7.2	<i>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.</i>		
CC7.2-01	Fusion has implemented third-party unified threat management and endpoint protection software (setup with automatic updates) on servers located in Chicago and Rolling Meadows offices and laptops to monitor for suspicious activities.	For a sample of servers and laptops, inquired of Fusion management and inspected a report from, and the dashboard of, the threat management and endpoint protection software, and the server configurations to determine that unified threat management and endpoint protection software was implemented and setup with automatic updates.	No exceptions noted.
CC7.2-02	For Fusion Framework® System™ components located in the production environment at Salesforce, Fusion relies on Salesforce's vulnerability and network monitoring tools that are setup to send alerts to the responsible person or team at Fusion.	Inquired of Fusion management and inspected the Salesforce SOC 2® report and Fusion management's review of that report to determine that Fusion relied on Salesforce's vulnerability and network monitoring tools that were setup to send alerts to the responsible person or team at Fusion.	No exceptions noted.
CC7.2-03	At least monthly, the Fusion Information Security Management Team reviews results from network	For a sample of months, inquired of Fusion management and inspected the minutes from the Fusion Information	No exceptions noted.

CC7.0: SYSTEM OPERATIONS

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
	vulnerability scans (using third-party unified threat management software) and vulnerabilities identified by the endpoint protection software and follows up on significant issues that are still open.	Security Management Team meetings with the vCISO and the remediation maintenance process books to determine that at least monthly, the Fusion Information Security Management Team reviewed results from network vulnerability scans (using third-party unified threat management software) and followed up on significant issues that were still open.	
CC7.2-04	As part of the risk management process, the Fusion Information Security Management Team considers whether additional tools or information resources are needed to meet Fusion Framework® System™ security objectives.	For a sample of weeks, inquired of Fusion management and inspected the current risk register and the minutes from the Fusion Information Security Management Team meetings with the vCISO to determine that as part of the risk management process, the Fusion Information Security Management Team considered whether additional tools or information resources were needed to meet Fusion Framework® System™ security objectives.	No exceptions noted.
CC7.2-05	As part of the risk management process, the Fusion Information Security Management Team considers if controls are adequate to mitigate identified risks and meet control objectives, while developing and implementing changes if needed.	For a sample of weeks, inquired of Fusion management and inspected the current risk register and the minutes from the Fusion Information Security Management Team meetings with the vCISO to determine that as part of the risk management process, the Fusion Information Security Management Team considered if controls were adequate to mitigate identified risks and meet control objectives, while developing and implementing changes if needed.	No exceptions noted.

CC7.0: SYSTEM OPERATIONS

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
CC7.3	<i>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.</i>		
CC7.3-01	For Fusion Framework® System™ components located in Chicago and Rolling Meadows, the Information Security Incident Management Policy and training presentation provide Fusion personnel and contractors with specific directions and responsibilities for reporting issues or incidents with the Fusion Framework® System™.	Inquired of Fusion management and inspected the Information Security Incident Management Policy and training presentations to determine that they provided Fusion personnel and contractors with specific directions and responsibilities for reporting issues or incidents with the Fusion Framework® System™.	No exceptions noted.
CC7.3-02	For Fusion Framework® System™ components located in the production environment at Salesforce, the Information Security Incident Management Policy provides Fusion personnel and contractors with specific directions and responsibilities for reporting issues or incidents with the Fusion Framework® System™.	Inquired of Fusion management and inspected the Information Security Incident Management Policy to determine that it provided Fusion personnel and contractors with specific directions and responsibilities for reporting issues or incidents with the Fusion Framework® System™.	No exceptions noted.
CC7.3-03	Weekly, the Fusion Information Security Management Team and the Internal IT Team meets with the vCISO to discuss the investigation and resolution of security incidents and breaches, if any.	For a sample of weeks, inquired of Fusion management and inspected the current risk register and the minutes from the Fusion Information Security Management Team meetings with the vCISO to determine that weekly, the Fusion Information Security Management Team and the Internal IT Team met with the vCISO to discuss the investigation and resolution of security incidents and breaches, if any.	No exceptions noted.

CC7.0: SYSTEM OPERATIONS

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
CC7.3-04	For Fusion Framework® System™ components located in the production environment at Salesforce, a member of the office of the CTO investigates and resolves issues, if any, relating to security vulnerabilities, incidents, or breaches as reported from Salesforce, Conga, or Okta, for which Fusion is responsible.	Inquired of Fusion management and inspected the security advisories from Salesforce, Conga, or Okta, the vulnerability trackers, the minutes from the Fusion Information Security Management Team meetings with the vCISO, and the remediation maintenance process books to determine that a member of the office of the CTO investigated and resolved issues, if any, relating to security vulnerabilities, incidents, or breaches as reported from Salesforce, Conga, or Okta, for which Fusion was responsible.	No exceptions noted.
CC7.4	<i>The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.</i>		
CC7.4-01	For Fusion Framework® System™ components located in Chicago and Rolling Meadows, the Information Security Incident Management Policy and training presentation provide Fusion personnel and contractors with specific directions and responsibilities for reporting issues or incidents with the Fusion Framework® System™.	Inquired of Fusion management and inspected the Information Security Incident Management Policy and training presentations to determine that they provided Fusion personnel and contractors with specific directions and responsibilities for reporting issues or incidents with the Fusion Framework® System™.	No exceptions noted.
CC7.4-02	For Fusion Framework® System™ components located in the production environment at Salesforce, the Information Security Incident Management Policy provides Fusion personnel and contractors with specific directions and responsibilities for reporting issues or incidents with the Fusion Framework® System™.	Inquired of Fusion management and inspected the Information Security Incident Management Policy to determine that it provided Fusion personnel and contractors with specific directions and responsibilities for reporting issues or incidents with the Fusion Framework® System™.	No exceptions noted.

CC7.0: SYSTEM OPERATIONS

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
CC7.4-03	Annually for Fusion Framework® System™ components located in the production environment at Salesforce, the Company engages a third-party to perform penetration testing of the Fusion application and critical and high vulnerabilities, if any, are remediated as needed.	Inquired of Fusion management and inspected the most recent penetration testing summary letter, the remediation maintenance process books, and minutes from the Fusion Information Security Management Team meetings with the vCISO to determine that penetration testing of the Fusion application was performed annually and critical and high vulnerabilities were remediated as needed.	No exceptions noted.
CC7.4-04	Fusion Framework® System™ domain controllers located in Chicago and Rolling Meadows offices are configured to be backed up daily to a NAS in the Chicago office.	Inquired of Fusion management and inspected the backup software configurations to determine that fusion Framework® System™ domain controllers located in Chicago and Rolling Meadows offices were configured to be backed up daily to a NAS in the Chicago office.	No exceptions noted.
CC7.4-05	Weekly, the Fusion Information Security Management Team and the Internal IT Team meets with the vCISO to discuss the investigation and resolution of security incidents and breaches, if any.	For a sample of weeks, inquired of Fusion management and inspected the current risk register and the minutes from the Fusion Information Security Management Team meetings with the vCISO to determine that weekly, the Fusion Information Security Management Team and the Internal IT Team met with the vCISO to discuss the investigation and resolution of security incidents and breaches, if any.	No exceptions noted.
CC7.4-06	For Fusion Framework® System™ components located in the production environment at Salesforce, a member of the office of the CTO investigates and resolves issues, if any, relating to security vulnerabilities, incidents, or	Inquired of Fusion management and inspected the security advisories from Salesforce, Conga, or Okta, the vulnerability trackers, the minutes from the Fusion Information Security Management Team meetings with	No exceptions noted.

CC7.0: SYSTEM OPERATIONS

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
	breaches as reported from Salesforce, Conga, or Okta, for which Fusion is responsible.	the vCISO, and the remediation maintenance process books to determine that a member of the office of the CTO investigated and resolved issues, if any, relating to security vulnerabilities, incidents, or breaches as reported from Salesforce, Conga, or Okta, for which Fusion was responsible.	
CC7.5	<i>The entity identifies, develops, and implements activities to recover from identified security incidents.</i>		
CC7.5-01	For Fusion Framework® System™ components located in Chicago and Rolling Meadows, the Information Security Incident Management Policy and training presentation provide Fusion personnel and contractors with specific directions and responsibilities for reporting issues or incidents with the Fusion Framework® System™.	Inquired of Fusion management and inspected the Information Security Incident Management Policy and training presentations to determine that they provided Fusion personnel and contractors with specific directions and responsibilities for reporting issues or incidents with the Fusion Framework® System™.	No exceptions noted.
CC7.5-02	For Fusion Framework® System™ components located in the production environment at Salesforce, the Information Security Incident Management Policy provides Fusion personnel and contractors with specific directions and responsibilities for reporting issues or incidents with the Fusion Framework® System™.	Inquired of Fusion management and inspected the Information Security Incident Management Policy to determine that it provided Fusion personnel and contractors with specific directions and responsibilities for reporting issues or incidents with the Fusion Framework® System™.	No exceptions noted.
CC7.5-03	As part of the risk management process, the Fusion Information Security Management Team considers if controls are adequate to mitigate identified risks and meet control objectives, while developing and implementing changes if needed.	For a sample of weeks, inquired of Fusion management and inspected the current risk register and the minutes from the Fusion Information Security Management Team meetings with the vCISO to determine that as part of the risk management process, the Fusion Information	No exceptions noted.

CC7.0: SYSTEM OPERATIONS

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
		Security Management Team considered if controls were adequate to mitigate identified risks and meet control objectives, while developing and implementing changes if needed.	
CC7.5-04	Weekly, the Fusion Information Security Management Team and the Internal IT Team meets with the vCISO to discuss the investigation and resolution of security incidents and breaches, if any.	For a sample of weeks, inquired of Fusion management and inspected the current risk register and the minutes from the Fusion Information Security Management Team meetings with the vCISO to determine that weekly, the Fusion Information Security Management Team and the Internal IT Team met with the vCISO to discuss the investigation and resolution of security incidents and breaches, if any.	No exceptions noted.
CC7.5-05	For Fusion Framework® System™ components located in the production environment at Salesforce, a member of the office of the CTO investigates and resolves issues, if any, relating to security vulnerabilities, incidents, or breaches as reported from Salesforce, Conga, or Okta, for which Fusion is responsible.	Inquired of Fusion management and inspected the security advisories from Salesforce, Conga, or Okta, the vulnerability trackers, the minutes from the Fusion Information Security Management Team meetings with the vCISO, and the remediation maintenance process books to determine that a member of the office of the CTO investigated and resolved issues, if any, relating to security vulnerabilities, incidents, or breaches as reported from Salesforce, Conga, or Okta, for which Fusion was responsible.	No exceptions noted.
CC7.5-06	Fusion Framework® System™ domain controllers located in Chicago and Rolling Meadows offices are configured to be backed up daily to a NAS in the Chicago office.	Inquired of Fusion management and inspected the backup software configurations to determine that fusion Framework® System™ domain controllers located in	No exceptions noted.

CC7.0: SYSTEM OPERATIONS

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
		Chicago and Rolling Meadows offices were configured to be backed up daily to a NAS in the Chicago office.	
CC7.5-07	For Fusion Framework® System™ components located in Chicago and Rolling Meadows, the backup software is configured to perform a data integrity check to ensure that data is able to be recovered in the event of data loss or integrity issues.	Inquired of Fusion management and inspected the backup software configurations and an example backup job results report to determine that for the backup software was configured to perform a data integrity check to ensure that data was able to be recovered in the event of data loss or integrity issues.	No exceptions noted.
CC7.5-08	For Fusion Framework® System™ components located in the production environment at Salesforce, Fusion relies on Salesforce's data backup, data restore and disaster recovery solutions.	Inquired of Fusion management and inspected the Salesforce SOC 2® report and Fusion management's review of that report to determine that Fusion relied on Salesforce's data backup, data restore and disaster recovery solutions.	No exceptions noted.

CC8.0: CHANGE MANAGEMENT

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
CC8.1	<i>The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.</i>		
CC8.1-01	Fusion has formally documented change management policies and procedures which are used to manage changes to Fusion Framework® System™ components.	Inquired of Fusion management and inspected the change management policies and procedures to determine that they were formally documented to manage changes to Fusion Framework® System™ components.	No exceptions noted.
CC8.1-02	Change requests related to Fusion Framework® System™ components are logged and managed in centralized ticketing systems.	Inquired of Fusion management and inspected the change management system dashboard to determine that change requests related to Fusion Framework® System™ components were logged and managed in centralized ticketing systems.	No exceptions noted.
CC8.1-03	As part of the risk management process, the Fusion Information Security Management Team considers whether changes are required to the Fusion Framework® System™ to maintain security commitments.	For a sample of weeks, inquired of Fusion management and inspected the current risk register and the minutes from the Fusion Information Security Management Team meetings with the vCISO to determine that as part of the risk management process, the Fusion Information Security Management Team considered whether changes were required to the Fusion Framework® System™ to maintain security commitments.	No exceptions noted.
CC8.1-04	A change request is created by Fusion management as deemed necessary depending on the significance and recurrence of identified risks or incidents.	For a sample of weeks, inquired of Fusion management and inspected the current risk register and the minutes from the Fusion Information Security Management Team	No exceptions noted.

CC8.0: CHANGE MANAGEMENT

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
		meetings with the vCISO to determine that a change request was created by Fusion management as deemed necessary depending on the significance and recurrence of identified risks or incidents.	
CC8.1-05	At least monthly, the Fusion Information Security Management Team reviews results from network vulnerability scans (using third-party unified threat management software) and vulnerabilities identified by the endpoint protection software and follows up on significant issues that are still open.	For a sample of months, inquired of Fusion management and inspected the minutes from the Fusion Information Security Management Team meetings with the vCISO and the remediation maintenance process books to determine that at least monthly, the Fusion Information Security Management Team reviewed results from network vulnerability scans (using third-party unified threat management software) and followed up on significant issues that were still open.	No exceptions noted.
CC8.1-06	For Fusion Framework® System™ components located in the production environment at Salesforce, a member of the office of the CTO investigates and resolves issues, if any, relating to security vulnerabilities, incidents, or breaches as reported from Salesforce, Conga, or Okta, for which Fusion is responsible.	Inquired of Fusion management and inspected the security advisories from Salesforce, Conga, or Okta, the vulnerability trackers, the minutes from the Fusion Information Security Management Team meetings with the vCISO, and the remediation maintenance process books to determine that a member of the office of the CTO investigated and resolved issues, if any, relating to security vulnerabilities, incidents, or breaches as reported from Salesforce, Conga, or Okta, for which Fusion was responsible.	No exceptions noted.
CC8.1-07	For changes to Fusion Framework® System™ components located in Chicago and Rolling Meadows, one or more	For a sample of change of Fusion Framework® System™ components located in Chicago and Rolling Meadows,	No exceptions noted.

CC8.0: CHANGE MANAGEMENT

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
	members of the CAB review the changes to ensure they were implemented in production as requested and planned.	inquired of Fusion management and inspected the help desk ticket and supporting documentation to determine that one or more members of the CAB reviewed the change to ensure it was implemented in production as requested and planned.	
CC8.1-08	For global changes to the Fusion Framework® System™ application located in the production environment at Salesforce, design documents and test plans are created and followed by the QA team.	For a sample of global changes to the Fusion Framework® System™ components located in the production environment at Salesforce, inquired of Fusion management and inspected the help desk tickets and supporting documentation to determine that design documents and test plans were created and followed by the QA team.	No exceptions noted.
CC8.1-09	For global changes to the Fusion Framework® System™ application located in the production environment at Salesforce, changes are tested in an environment separate from production.	For a sample of global changes to the Fusion Framework® System™ components located in the production environment at Salesforce, inquired of Fusion management and inspected the help desk tickets and supporting documentation to determine that they were tested in an environment separate from production.	No exceptions noted.
CC8.1-10	For global changes to the Fusion Framework® System™ application located in the production environment at Salesforce, changes are reviewed and approved by the CAB prior to implementation in production.	For a sample of global changes, inquired of Fusion management and inspected the help desk tickets and supporting documentation to determine that they were reviewed and approved by the CAB prior to implementation in production.	No exceptions noted.

CC8.0: CHANGE MANAGEMENT

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
CC8.1-11	Fusion Framework® System™ software developers do not have update access to the production environment at Salesforce unless granted access by an authorized Fusion customer representative.	For a sample of months, inquired of Fusion management and inspected the help desk tickets of Fusion management's monthly review of logical user access, and correspondence from Fusion management to determine that Fusion Framework® System™ software developers did not have update access to the production environment at Salesforce unless granted access by an authorized Fusion customer representative.	No exceptions noted.
CC8.1-12	A version control library is used to store Fusion Framework® System™ software code and to manage the development process. Only authorized Fusion personnel have access to the version control library.	Inquired of Fusion management and inspected the version control software user access list and Fusion management's review to determine that it was used to store Fusion Framework® System™ software code and to manage the development process, and only authorized Fusion personnel had access to it.	No exceptions noted.
CC8.1-13	For Fusion Framework® System™ existing customer post-implementation change requests, Fusion makes the requested change (if not executed by the customer) only upon being authorized to do so by the customer as submitted through the Fusion Salesforce case system.	For a sample of customer post-implementation changes, inquired of Fusion management and inspected the statements of work to determine that they were authorized by the customer.	No exceptions noted.

CC9.0: RISK MITIGATION

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
CC9.1	<i>The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.</i>		
CC9.1-01	The Fusion Information Security Management Team has established a formal risk management process for managing Fusion Framework® System™ security risks.	For a sample of weeks, inquired of Fusion management and inspected the current risk register and the minutes from the Fusion Information Security Management Team meetings with the vCISO to determine that the Fusion Information Security Management Team established a formal risk management process for managing Fusion Framework® System™ security risks.	No exceptions noted.
CC9.1-02	As part of the risk management process, the Fusion Information Security Management Team assesses risk and assigns ratings based on factors such as likelihood and magnitude for the purpose of prioritizing risk treatment plans.	For a sample of weeks, inquired of Fusion management and inspected the current risk register and the minutes from the Fusion Information Security Management Team meetings with the vCISO to determine that as part of the risk management process, the Fusion Information Security Management Team assessed risk and assigned ratings based on factors such as likelihood and magnitude for the purpose of prioritizing risk treatment plans.	No exceptions noted.
CC9.1-03	Annually for the Fusion Framework® System™ components located in Chicago and Rolling Meadows, the Company engages a third-party to perform penetration testing and Internal IT responds to issues identified.	Inquired of Fusion management and inspected the most recent penetration testing reports, the remediation maintenance process books, and minutes from the Fusion Information Security Management Team meetings with the vCISO to determine that penetration testing of the Fusion Framework® System™ components located in	No exceptions noted.

CC9.0: RISK MITIGATION

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
		Chicago and Rolling Meadows was performed annually and Internal IT responded to issues identified.	
CC9.1-04	Annually for Fusion Framework® System™ components located in the production environment at Salesforce, the Company engages a third-party to perform penetration testing of the Fusion application and critical and high vulnerabilities, if any, are remediated as needed.	Inquired of Fusion management and inspected the most recent penetration testing summary letter, the remediation maintenance process books, and minutes from the Fusion Information Security Management Team meetings with the vCISO to determine that penetration testing of the Fusion application was performed annually and critical and high vulnerabilities were remediated as needed.	No exceptions noted.
CC9.1-05	For Fusion Framework® System™ components located in the production environment at Salesforce, Fusion relies on Salesforce's data backup, data restore and disaster recovery solutions.	Inquired of Fusion management and inspected the Salesforce SOC 2® report and Fusion management's review of that report to determine that Fusion relied on Salesforce's data backup, data restore and disaster recovery solutions.	No exceptions noted.
CC9.1-06	Annually, Fusion management reviews the redundant site switching exercise performed by Salesforce and determines if any changes to the Fusion Framework® System™ are necessary to maintain security commitments.	Inquired of Fusion management and inspected the remediation maintenance process book to determine that Fusion management reviewed the redundant site switching exercise performed by Salesforce and determined if any changes to the Fusion Framework® System™ were necessary to maintain security commitments.	No exceptions noted.
CC9.2	<i>The entity assesses and manages risks associated with vendors and business partners.</i>		

CC9.0: RISK MITIGATION

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
CC9.2-01	For Fusion vendors that require their employees to have logical or physical access to Fusion Framework® System™ components, Fusion management assigns a Fusion employee to monitor and oversee the vendor employee's activities.	For a sample of new vendor employees that required logical or physical access to a Fusion Framework® System™ component, inquired of Fusion management and inspected the vendor MSA, SOW, or the vendor employee profile to determine that Fusion management assigned a Fusion employee to monitor and oversee the vendor employee's activities.	No exceptions noted.
CC9.2-02	For Fusion vendors that require their employees to have logical or physical access to Fusion Framework® System™ components, either an MSA, a non-disclosure agreement ("NDA"), or other agreement that includes data/asset protection responsibilities prior to commencing work is required.	For a sample of new vendors, inquired of Fusion management and inspected the vendor agreements to determine that they included data/asset protection responsibilities and were obtained prior to the vendor commencing work.	No exceptions noted.
CC9.2-03	For vendor employees that require logical or physical access to Fusion Framework® System™ components, background check (or equivalent) is required.	For a sample of new vendor employees that required logical or physical access to a Fusion Framework® System™ component, inquired of Fusion management and inspected the background check or the requirement to obtain background check in the vendor agreement to determine that background checks were obtained.	No exceptions noted.
CC9.2-04	For vendors that have significant interaction with the Fusion Framework® System™, the Fusion Information Security Management Team performs a vendor risk assessment.	For a sample of new vendors, inquired of Fusion management and inspected the vendor risk assessment procedures performed and results to determine that the Fusion Information Security Management Team performed a vendor risk assessment.	No exceptions noted.

CC9.0: RISK MITIGATION

CNTL #	Description of Fusion's Controls	FGMK's Tests of Controls	Results of FGMK's Tests of Controls
CC9.2-05	Annually, Fusion management obtains and reviews SOC reports from each subservice organization to identify if there are issues noted that would potentially impact Fusion Framework® System™ security objectives.	Inquired of Fusion management and inspected each subservice organization's SOC 2® report, bridge letter (if applicable), and Fusion management's review of those reports and bridge letters to determine that annually, Fusion management obtained and reviewed them to identify if there were issues noted that would potentially impact Fusion Framework® System™ security objectives.	No exceptions noted.

Section 5

Other Information Provided by Fusion

Other Information Provided by Fusion

Fusion Management's Responses to FGMK Testing Exceptions

Fusion management is providing the following information in response to the SOC 2® examination performed by our service auditor, FGMK, for the period July 1, 2020 to June 30, 2021. The information below provides additional background on certain exceptions identified by FGMK, and our plan for remediation. Fusion management takes these findings seriously and has either already implemented corrective measures or has developed remediation plans that will be implemented according to priority.

Control No.	Description of Fusion's Controls	Results of FGMK's Tests of Controls	Fusion Management's Response
CC1.4-03	Fusion policy requires background checks and drug testing for Fusion personnel and contractors to be initiated prior to employment or engagement start date.	<u>New Personnel</u> Exception noted. For 1 of 10 new personnel selected for testing, that background check was initiated 1 week after start date. <u>New Contractors</u> No exceptions noted.	The background check was initiated before the employee was provided with access to any systems. The onboarding procedures have been reviewed, and additional checks have been added to prevent future occurrences.

Control No.	Description of Fusion's Controls	Results of FGMK's Tests of Controls	Fusion Management's Response
CC2.2-04	Fusion personnel and contractors are required to attend security awareness training within two weeks of hire and annually thereafter.	<u>New Personnel</u> Exception noted. For 1 of 10 personnel selected for testing, security awareness training was attended about 4 weeks after hire date. <u>New Contractors</u> No exceptions noted. <u>Annual Training</u> No exceptions noted.	The security awareness training for a new employee was delayed so this employee could utilize a new training module. We have updated our onboarding procedures to ensure that security awareness training is completed on time.
CC6.2-03 CC6.3-03	Monthly, the Directory of Security reviews Okta user accounts (including administrator accounts) to ensure access is limited to authorized Fusion users as needed.	Exceptions noted. For 4 of 4 months selected for testing, the help desk tickets indicated that user accounts were compared to the HR listing of active Fusion personnel, however, review of Okta administrator access was not documented.	The administrative access review is part of the review process. The associated procedures have been updated to ensure that the results of the periodic reviews provide detailed documentation.
CC6.4-04	Physical access to the Fusion office suites, server room, and server cage is removed within the timeframe as requested by Fusion management.	Exceptions noted. For 3 of 5 separations, physical access was revoked 3 days, 6 days, and 22 days after the separation and request date.	Management has updated the offboarding procedures to ensure that physical access is deactivated in time. Furthermore, a subsequent review of the access logs did not indicate any unauthorized physical access.

Control No.	Description of Fusion's Controls	Results of FGМК's Tests of Controls	Fusion Management's Response
CC6.8-01	The ability to install software or make configuration changes to servers and firewalls in Chicago and RMO offices, and laptops is restricted to authorized Fusion IT personnel.	<p><u>Servers and Firewalls</u> No exceptions noted.</p> <p><u>Laptops</u> Exceptions noted. For 2 of 41 laptops selected for testing, temporary administrator accounts (1 on each laptop, with ability to install software or make configuration changes) were present. FGМК inquired of Fusion management to determine that they were authorized, and they were setup for specific, short-term needs. However, the approvals of that temporary administrator access were not available.</p> <p>Subsequent to FGМК's testing, Fusion removed these 2 accounts on these 2 laptops and FGМК inspected screen prints to determine that they were removed.</p>	The temporary administrative access to both users was authorized and granted by a Fusion's Information Technology team member. The tickets did not capture detailed accounts of the processes. We have discussed with the control performers to ensure that all future tickets capture needed details.