COALFIRE CONTROLS

Report on Certinia Inc.'s Certinia Services Relevant to Security and Confidentiality Throughout the Period November 1, 2022 to October 31, 2023

SOC 3® - SOC for Service Organizations: Trust Services Criteria for General Use Report

certinia

formerly FinancialForce

Table of Contents

Section 1

Independent Service Auditor’s Report

Independent Service Auditor's Report

To: Certinia Inc. ("Certinia")

Scope

We have examined Certinia's accompanying assertion titled "Assertion of Certinia Inc. Management" (assertion) that the controls within the Certinia Services (system) were effective throughout the period November 1, 2022 to October 31, 2023, to provide reasonable assurance that Certinia's service commitments and system requirements were achieved based on the trust services criteria relevant to security and confidentiality (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* (2017 TSC).

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

Certinia uses a subservice organization to provide infrastructure support and management, physical security, backup and recovery functions to maintain the information systems. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Certinia, to achieve Certinia's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of Certinia's controls. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The information included in attachment C, "Other Information Provided by Certinia Inc. That Is Not Covered by the Service Auditor's Report," is presented by Certinia's management to provide additional information and is not a part of Certinia's description of the boundaries of the system. Information included in attachment C has not been subjected to the procedures applied in the examination and, accordingly, we express no opinion on it.

Service Organization's Responsibilities

Certinia 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 Certinia's service commitments and system requirements were achieved. Certinia has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Certinia is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. 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 management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve Certinia's service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Certinia's service commitments and system requirements based on the applicable trust services criteria.

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

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the 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.

Opinion

In our opinion, management's assertion that the controls within the Certinia Services were effective throughout the period November 1, 2022 to October 31, 2023, to provide reasonable assurance that Certinia'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 Certinia's controls operated effectively throughout that period is fairly stated, in all material respects.

Coalfire Controls LLC

Greenwood Village, Colorado
December 21, 2023

Section 2

Assertion of Certinia Inc. Management

Assertion of Certinia Inc. (“Certinia”) Management

We are responsible for designing, implementing, operating and maintaining effective controls within the Certinia Services (system) throughout the period November 1, 2022 to October 31, 2023, to provide reasonable assurance that Certinia’s service commitments and system requirements were achieved based on the trust services criteria relevant to security and confidentiality (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* (2017 TSC). Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our assertion.

The description of the boundaries of the system indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Certinia, to achieve Certinia’s service commitments and system requirements based on the applicable trust services criteria.

Certinia uses a subservice organization for infrastructure support and management, physical security, backup and recovery functions to maintain the information systems. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Certinia, to achieve Certinia’s service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of Certinia’s controls. The description of the boundaries of the system does not disclose the actual controls at the subservice organization.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period November 1, 2022 to October 31, 2023, to provide reasonable assurance that Certinia’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 Certinia’s controls operated effectively throughout that period. Certinia’s objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in attachment B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period November 1, 2022 to October 31, 2023 to provide reasonable assurance that Certinia’s service commitments and system requirements were achieved based on the applicable trust services criteria.

Certinia Inc.

Attachment A

Certinia Inc.’s Description of the Boundaries of Its Certinia Services

Type of Services Provided

Certinia Inc. (“Certinia” or “the Company”) is a cloud business applications company that provides software services for enterprise resource planning, professional services organizations, customer success organizations, and human capital management on the Lightning platform, a cloud computing platform provided by Salesforce. These software services are collectively referred to as “Certinia Services.”

Certinia serves its clients (or user entities) from its corporate headquarters in San Jose, California; its Asia Pacific region headquarters in Sydney, Australia; and its Europe, Middle East, and Africa (EMEA) region headquarters in Harrogate, United Kingdom.

Certinia Services use Salesforce’s proprietary Lightning platform, which includes tools for development, reporting, workflow authorizations, dashboards, social media (Chatter), and integration, as its underlying technology. Salesforce provides and manages the Lightning platform, performing back-ups, providing access and authorization capability, managing performance, implementing anti-virus measures, and ensuring platform security. More information on the Lightning platform and its certifications is available here: https://compliance.salesforce.com/en and here: https://www.salesforce.com/campaign/lightning/.

As native Lightning platform applications, the Certinia Services and Salesforce applications are embedded together, which helps simplify user adoption, streamline business processes, improve reporting, and enable cross-training between functions. Customers are responsible for configuring their implementation of Certinia Services and the Lightning platform and managing their organization’s instance(s) of the Lightning platform and installed applications. Additionally, customers are responsible for configuring the controls available within the Lightning platform for their security and compliance requirements (e.g., provisioning and monitoring access of their instances).

Enterprise Resource Planning Services

The Certinia Services’ Enterprise Resource Planning suite of services includes Accounting, Revenue Recognition, Billing Central, Order Procurement and Inventory (OPI), Financial Planning and Analysis, and Reporting and Analytics.

Accounting

Accounting is used to manage user entities’ finance and accounting processes with components including modules for processing sales ordering, billing, accounts receivable, collections, the general ledger, accounts payable, and fixed asset management. Accounting is a real-time accounting system that is based on a unified ledger design. This means that transactions that are posted to the ledger must have balancing debit and credit lines, so the ledger always balances.

Accounting includes components for multi-currency, multi-tax, and multi-company accounting and is built for both financial statement generation and real-time financial analysis. The system is furnished with financial report templates and customizable dashboards that can be accessed from an internet browser or mobile device.

From a financial perspective, integration with Salesforce allows the opportunity-to-cash process to flow seamlessly and securely through sales, billing, and receivables without manual effort, special integrations, or extraneous spreadsheets. This allows users the ability to see complete views of their customers’ information, including opportunities, cases, invoices, credits, and cash payments, without performing any special synchronization or master data management routines.

Revenue Recognition

Revenue Recognition helps user entities handle their revenue recognition needs by providing a number of standard templates and the ability to define revenue recognition rules. Revenue Recognition allows users to:

- Identify revenue recognition events to create revenue recognition transactions
- Choose from predefined revenue recognition calculations
- Recalculate revenue schedules at any time
- Export journal information
- Provide reports and dashboards showing revenue recognition actuals
- Allocate recognized revenue across several accounts
- Automate the calculation and management of revenue recognition
- “Plug and play” by using standard revenue recognition templates to address common revenue recognition scenarios

Revenue Recognition also leverages the Lightning platform offerings, making it possible to extend and build out functionality to handle more complex revenue recognition needs.

Billing Central

Billing Central helps user entities manage complex customer billing requirements on the Lightning platform, integrating with the activities of sales, services, customer support, and customer success staff. Billing Central accommodates a variety of billing structures and models, including subscription- and usage-based billing. With Billing Central, user entities can use one screen and process to configure and manage pricing and contract terms, which reduces the need for integrations with other business applications. This helps create a single source of business truth, improves accuracy, and enhances efficiency across the billing life cycle. With Billing Central, user entities can manage:

- Flexible pricing structures and quantity breaks
- Use of plans to package or bundle products
- Creation, modification, and renewal of contracts
- Automation of billing operations and taxation

Order Procurement and Inventory

OPI is a portfolio of applications used to execute the buying and selling of goods and services. Created to support the business models of distributors and value-added resellers (VARs) for their quote-to-cash and procure-to-pay business processes, OPI includes the following modules: Configure Price Quote, Order Fulfillment, Service Contracts, Invoicing, Inventory Management, Procurement, and Fixed Assets.

OPI is designed to support multiple fulfillments, procurements, and revenue streams with complex business processes, exposing deal profitability, and to provide businesses with instrumented information to monitor key performance indicators of their business.

OPI is also designed to help organizations efficiently manage their spending, customer orders, and inventory management in one integrated set of applications. When in use with the Accounting, Revenue Recognition, and Professional Services Automation (PSA) applications, OPI can provide a comprehensive solution for firms that provide both goods and services to their customers.

Financial Planning and Analysis

Certinia Financial Planning and Analysis, also known as “Budgeting,” allows users to generate, create, and modify their budgets with a combination of Salesforce Platform tools and the use of Microsoft Excel files. Intelligent calculations and formulas can also be included to aid in the creation of different budget scenarios.

To simplify integrations, the Financial Planning and Analysis solution has been designed to be integrated with Certinia Accounting so that budgets can be based on historical transactions from a prior year. Certinia Financial Planning and Analysis can also be integrated with other solutions.

Flexible configurations have been included to allow both bottom-up and top-down budgets or forecasts to be created with Salesforce platform features supporting approvals and security.

Reporting and Analytics

The Reporting and Analytics suite of services includes Financial Report Builder (FRB), Business Analytics, Certinia Statements, and Certinia Reporting.

Financial Report Builder

FRB allows users to build structured reports based on both simple and complex criteria. Primarily built to aid Certinia Accounting customers in building their statements, FRB uses Salesforce Analytics datasets from any data source so that multiple departments can be serviced. FRB allows users to add sections, columns, and filters to their reports. The Salesforce Analytics platform (Tableau CRM) supports aggregation of up to 10 billion records.

FRB offers insight into the numbers on reports through drill-down functionality, detailing the transactions that form a result and then down into the source record itself. Results can also be exported as a CSV.

Business Analytics

Certinia Business Analytics provides users with access to several analytics dashboards sourced from every application in the Certinia product suite. This includes Certinia Accounting, PSA, Billing Central, Revenue Management, and Supply Chain. Using the Salesforce Tableau CRM platform, Business Analytics allows users to view different areas of the business and drill down into records to perform actions. Many of the dashboards provided can also be accessed through mobile devices for both Android and iOS.

Analysis areas include trending prediction dashboards for revenue and gross margin, plus dashboards to aid with the capacity and demand planning of resources. All dashboards are designed to complement and enhance the products they are built on. The results can be shared through Chatter, Quip, and Microsoft Excel.

In addition, advanced AI through use of the Salesforce Einstein Discovery platform can be applied to historical records to provide insight into not just what happened but predictions into what will happen, why it happened, and prescriptive insight into what can be done to improve outcomes.

Financial Statements

Certinia Financial Statements provides users with a subset of Business Analytics’ functionality in order to make the building of Financial Statements with Salesforce Analytics accessible to all Certinia Accounting users. When used in combination with Financial Report Builder, users can benefit from the volume and performance of the Salesforce Analytics (Tableau CRM) platform to build statutory reports.

Certinia Reporting

Certinia Reporting produces formatted statutory financial reports using information from Certinia Accounting. The Certinia Reporting offering produces reports suitable for presentation, enables the use of out-of-the-box reports, and provides the ability to build customer reports for multiple departments.

Professional Services Organizations Services and Customer Success Organizations Services

The Professional Services Organization Services (“PS Cloud”) and the Customer Success Organization Services (“CS Cloud”) includes PSA, Customer Success Operations (CS Ops) Cloud, and Services CPQ.

PSA

PSA is used to manage billable projects, professional resources, time and expense entries, and project accounting. Like FM, PSA is built natively and remotely hosted on the Lightning platform. PSA is designed to help user entities manage their people, customers, projects, and financials in one integrated services management application, thereby helping them deliver projects on time, within scope, and under budget while improving employee utilization and project profitability.

The Lightning platform enables Certinia to leverage a variety of mobile devices, customer portals, workflow engines, and analytics tools that provide 24/7 support to service-oriented businesses. These include Chatter, a social media application that brings collaboration functionality to project delivery. Chatter allows sales and project team members to create project-specific Chatter groups and discussion streams that can become integral to a project’s success.

PSA is also designed to provide service managers visibility into the services pipeline, the demand for resources, target start dates, customer interactions, active projects, issues and risks, and billing details, as well as provide a single view of the customer.

Customer Success Operations Cloud

CS Ops Cloud uses the Salesforce platform to organize and orchestrate the implementation of a client’s customer success best practices end-to-end and enterprise-wide. CS Ops simplifies and systematizes essential customer success activities, giving stakeholders a repeatable, predictable way to gain complete control over their CS initiatives.

By displaying a complete, coordinated picture of the entire customer life cycle, CS Ops Cloud allows collaboration across teams. The platform enables stakeholders across the organization to collaborate, derive key insights, and take actions that increase customer satisfaction, retention, expansion, and referrals.

Services CPQ

Services CPQ helps clients with the services estimation process, providing a single workspace that enables a dedicated estimating team or project or delivery managers to quote services. Services CPQ offers clients the ability to:

- Initiate the estimating process from an opportunity
- Build up a quote quickly and accurately from the bottom up or from client-defined templates
- Create templates containing resource requests and/or tasks
- Analyze “what if” scenarios around resources, expenses, and margin requirements

- Manage discounts
- Initiate required approval processes (using platform approval process capabilities)
- Feed the final estimate directly to the opportunity in customer relationship management (CRM) or into the Salesforce CPQ process, if needed
- Create resource demand at the opportunity to support resource forecasting needs
- Create a PSA project from the estimate

Human Capital Management (HCM)

HCM allows user entities to manage their human resources (HR) through a unified, cloud-based solution on the Lightning platform that supports the entire employee life cycle. Functional areas of HCM include:

- A core HR information system to manage worker data
- Applicant tracking system for recruitment
- Employee and manager self-service
- Performance management goal setting and reviews
- Healthcare benefit administration and enrollment
- Compensation planning
- Training and development
- Time and attendance management
- Payroll connect to any payroll service bureau
- Reporting and analytics

HCM includes Chatter, which allows collaboration in employee interactions and the building of company culture. HCM is integrated with the PSA application, allowing for worker automation for users of both products.

HCM can be used across the organization. It enables company leaders to make business decisions by providing visibility into their worker data, alleviates administrative tasks from HR and managers, and offers self-service capability and social tools to employee users.

Configurability

The Certinia Services are configurable, flexible, and suitable to a variety of types and sizes of user entities across different industry segments. The Lightning platform allows users to add fields and objects and to build their own applications alongside Certinia Services, which are also configurable. The combined flexibility of Certinia Services and the Lightning platform typically requires users to purchase consulting services from Certinia or its consulting partners to assist with implementations. The range and amount of consulting services required by each user entity varies based on the complexity of the implementation and the skills of the user entity. Note that configuration and implementation services are contracted separately and are not within the scope of this report.

Customer Support and Maintenance

Certinia is responsible for developing, maintaining, and supplying the applications for deployment within user entities' Salesforce tenants. As needed, Certinia improves the applications and makes new releases

available to user entities. Certinia also supplies Customer Support to answer questions about its applications and assist with any issues a user may experience. The support service includes:

- *Online Support*: Users can obtain online help directly from a Certinia application. Users also have access to the Certinia Community, an online destination that allows users to log cases, find answers, and log ideas on product enhancements.
- *Standard Support*: Users obtain direct access to the Customer Support team by phone or via Community support cases.
- *Premier Support*: For an additional fee, users can obtain faster response times, prioritized escalation and a dedicated resource to manage cases (includes the features of Online and Standard Support).

The Components of the System Used to Provide the Services

The boundaries of Certinia Services are the specific aspects of the Company's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of Certinia Services.

The components that directly support the services provided to customers are described in the subsections below.

Infrastructure

To maintain the information systems, Certinia uses a third party to provide infrastructure, as well as platform, physical security, and backup and recovery functions.

The in-scope hosted infrastructure also consists of multiple supporting tools to address the following business functions:

- Customer data storage
- Certinia instance of Salesforce

Software

Software consists of the programs and software that support Certinia Services (operating systems [OSs], middleware, and utilities). The list of software and ancillary software used to build, support, secure, maintain, and monitor Certinia Services includes applications to support the following functions:

- Application infrastructure, auditing and logging, security incident case tracking, procurement, metrics
- Vulnerability management (used for internal Company asset vulnerability scanning)
- Anti-virus (used for internal Company endpoint security)
- Protection against threats on the internet
- Helpdesk ticketing system
- Bug tracker

- Integration and building
- Static code analysis
- Source control
- Multi-factor authentication
- Secure backup and endpoint data leakage prevention
- Centralized logging, alerting, and security monitoring
- Internal Company attack surface management tool for measuring and detecting infrastructure issues
- Private bug bounty platform to allow independent security researchers to report vulnerabilities at *.certinia.com
- Identity and access management
- Identity Platform
- Password Manager
- Security training and awareness platform
- Compliance training platform
- Vendor risk management platform
- Productivity and email
- Third-party MSSP

People

The Company develops, manages, and secures Certinia Services via separate departments. The responsibilities of these departments are defined in the following table:

People	
Group/Role Name	**Function**
Executive Leadership Team (ELT)	Responsible for overseeing company-wide activities, establishing and accomplishing goals, and overseeing objectives.
Research & Development (R&D)	Responsible for the technical design, development, testing, and release of Company applications, including enhancements and changes to the applications.
Professional Services	Responsible for implementing and customizing the services for certain Company customers.
Product Management	Responsible for overseeing the product life cycle, including adding new product functionality.
Human Resources (HR)	Responsible for onboarding new personnel, defining the roles and positions of new hires, performing background checks, and facilitating the employee termination process.
Employee Success	Responsible for the support, strategic development, and accompanying administration of the Company's workforce.

People	
Group/Role Name	**Function**
Finance	Responsible for the invoicing of Company services, payment of suppliers, and budgeting, as well as for producing the management accounts.
IT Operations	Responsible for the internal information technology (IT) infrastructure, internal software-as-a-service (SaaS) applications, and endpoint devices used by the Company to develop and support Certinia Services.
Information Security	Responsible for the Company's information security program, helping ensure that customer and Company information assets are adequately protected.
Legal	Responsible for overseeing legal, compliance, contracts, and corporate governance matters at the Company.

Procedures

Procedures include the automated and manual procedures involved in the operation of Certinia Services. Procedures are developed and documented by the respective teams for a variety of processes, including those relating to product management, engineering, technical operations, security, IT, and Employee Success. These procedures are drafted in alignment with the overall information security policies and are updated and approved as necessary for changes in the business, but no less than annually.

The following table details the procedures as they relate to the operation of Certinia Services:

Procedures	
Procedure	**Description**
Logical and Physical Access	How the Company restricts logical and physical access, provides and removes that access, and prevents unauthorized access.
System Operations	How the Company manages the operation of the system and detects and mitigates processing deviations, including logical and physical security deviations.
Change Management	How the Company identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made.
Risk Mitigation	How the Company conducts risk mitigation activities, including performing an annual risk assessment, and prioritizes risks as identified by business and functional stakeholders.

Data

Data refers to transaction streams, files, data stores, tables, and output used or processed by the Company. The customer or end-user defines and controls the data they load and store in their Salesforce production instance via the Lightning platform. This data is loaded into the environment and accessed remotely from customer systems over a secure browser via the internet.

Customer data is managed, processed, and stored within Salesforce in accordance with relevant data protection and other regulations and with specific requirements formally established in customer contracts.

As part of Certinia Services, customers can limit access to confidential or sensitive information by configuring the Salesforce platform for secure methods and protocols.

Subservice Organization

The Company uses a subservice organization to provide infrastructure support and management, physical security, backup and recovery functions to maintain the information systems. The Company's controls related to Certinia Services cover only a portion of the overall internal control for each user entity of Certinia Services. The description does not extend to the colocation services for IT infrastructure provided by the subservice organization.

Although the subservice organization has been carved out for the purposes of this report, certain service commitments, system requirements, and applicable criteria are intended to be met by controls at the subservice organization.

Company management receives and reviews the subservice organization's SOC 2 report annually. In addition, through its operational activities, Company management monitors the services performed by the subservice organization to determine whether operations and controls expected to be implemented are functioning effectively. Management also communicates with the subservice organization to monitor compliance with the service agreement, stay informed of changes planned at the hosting facility, and relay any issues or concerns to management of the subservice organization.

Complementary User Entity Controls

Complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Certinia, to achieve Certinia's service commitments and system requirements based on the applicable trust services criteria.

Attachment B

Principal Service Commitments and System Requirements

Principal Service Commitments and System Requirements

Commitments are declarations made by management to customers regarding the performance of Certinia Services. Commitments are communicated in the Company's Master Subscription Agreement (MSA) and Data Processing Addendum, which are posted to the Certinia website here: https://certinia.com/legal/msa/ and https://certinia.com/privacy/, respectively.

System requirements are specifications regarding how Certinia Services should function to meet the Company's principal commitments to user entities. System requirements are specified in the Company's policies and procedures.

The Company's principal service commitments and system requirements related to Certinia Services include the following:

Trust Services Category	Service Commitments	System Requirements
Security	• The Company will maintain administrative and technical safeguards for protecting the security and confidentiality of customer data. • The Company will maintain security incident management policies and procedures and will notify the customer without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to customer data, including personal data, transmitted, stored, or otherwise processed by the Company or its sub-processors.	• Logical access standards • Employee provisioning and deprovisioning standards • Access review standards • Incident handling standards • Risk and vulnerability standards • Logging standards • Anti-malware standards
Confidentiality	• The Company will maintain all customer data as confidential and will not use or disclose information to any unauthorized parties without written consent. • The Company will use the same, but no less than reasonable, degree of care that it uses to protect the confidentiality of its own confidential information.	• Data classification standards • Retention and destruction standards • Data handling standards

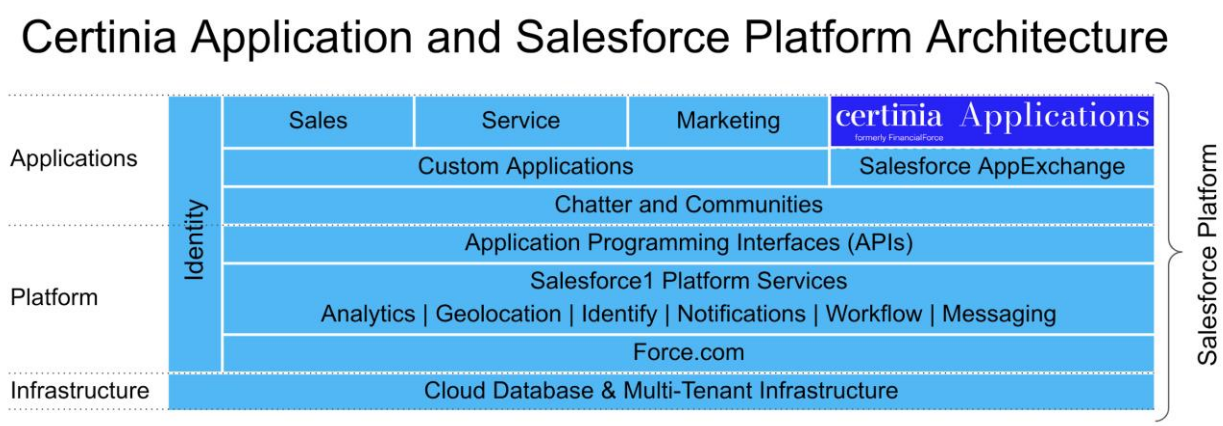
Attachment C

Other Information Provided by Certinia Inc. That is Not Covered by the Service Auditor's Report

Introduction

As a 100% native force application all Customer Data processed by Certinia applications reside on the Salesforce cloud platform owned, operated and managed by Salesforce. Salesforce provides a public SaaS offering. Certinia provides apps but no infrastructure. Salesforce provides the data center and customer data is stored at Salesforce. As such, the majority of the infrastructure, network, and platform security controls are inherited and implemented at Salesforce.

You can find an overview of our Information Security Program, including our shared security services with Salesforce, through the various collateral and security documents we make available through our vendor risk management platform - Whistic. This diverse range of resources are quintessential for understanding Certinia products and security, especially for those who may be new to the Salesforce platform and the concept of applications natively built on Salesforce.



Built on the Salesforce Platform - Salesforce Security

Certinia applications were developed on Force.com, an industry-leading and mature platform for cloud applications provided by Salesforce. Certinia applications listed on AppExchange go through a qualitative and quantitative security review process with Salesforce to ensure applications meet a set of security standards and best practices. Learn more about security at Salesforce through the link below.

Link: https://certinia.com/legal-privacy-trust/trust/salesforce-security/

Whistic Public Profile

To help you gain a better understanding of Certinia security, we have partnered with Whistic to provide you with more information about information security at Certinia and the security of our products and services. It's a one stop shop for finding all of the latest and greatest of our publicly available security resources.

Link: https://certinia.com/trust/security-profile/

Security Whitepaper

Certinia's Information Security Team has prepared a formal, publicly-facing security whitepaper. This document is a high-level overview in narrative format which covers several key areas, inclusive of these areas:

- Security Overview
- Shared Security Responsibilities Model
- Certifications and Attestations
- Infrastructure Security
- Product Security
- Data Encryption
- Application Controls
- Disaster Recovery
- Change Management
- Incident Management

Link: https://certinia.com/wp-content/uploads/2023/06/Certinia-Security-Whitepaper.pdf

Information Security Frequently Asked Questions

Have a question and want a quick answer? Using the most asked questions and topics we see from customer questionnaires, Certinia's Information Security Team has compiled a publicly-facing FAQs document. This document was designed as a quick to navigate document, answering the majority of the most-asked questions from customers relevant to the following areas:

- Architecture and Data Flow Overview
- Major Compliance Reports and Frameworks
- Network and Infrastructure Security
- Backups and Encryption
- Business Continuity and Disaster Recovery
- Access and Authentication
- Incident Management
- Change Management and Product Security
- IS Governance, Risk, and Compliance

Link: https://certinia.com/wp-content/uploads/2023/06/Certinia-Information-Security-FAQ.pdf

CSA CAIQ - STAR Level 1 Assessment

The Cloud Security Alliance - Consensus Assessments Initiative Questionnaire, or CSA CAIQ, is a comprehensive, publicly-facing, industry-standard self-assessment questionnaire published by the CSA. This assessment helps distinguish ownership (or shared ownership) of the controls and responsibilities between the service provider (Certinia), service customer (Customer), and third parties (Salesforce, who provides the required platform infrastructure). Given that Certinia applications require the Salesforce platform which presents several differences from a traditional architecture, the CSA CAIQ is an invaluable resource for understanding the responsibilities and controls fulfilled by each party.

Link: https://cloudsecurityalliance.org/star/registry/certinia/services/certinia-cloud-applications/

Full Whistic Security Profile - Confidential Documents, Audits, and Reports

Certinia has numerous security documents classified as confidential that are made only available to current customers as well as prospective customers under NDA. All of our security documents are shared securely through our access-restricted Full Whistic Security Profile. Access to the full profile can be requested through your AE / CSM.

Our Full Whistic Security Profile includes continuous access to our latest documents in real-time. These include:

- SOC 1 Type II Report
- SOC 2 Type II Report
- Bridge / Gap Letters for our SOC Reports (letters are issued quarterly)
- Annual Penetration Test Report
- VSA Questionnaire
- SIG Lite Questionnaire
- Cyber Insurance
- Certinia Architecture and Performance Overview
- Information Security Policies
  - Security Policy and Standards
  - IS Program Charter
  - Cyber Security Incident Response Plan (CSIRP)
  - Security Incident Management Procedure
  - Secure SDLC Policy
  - Threat and Vulnerability Management Guideline
  - Security Awareness and Training Guideline
  - IS Data Classification Policy
  - Vendor Risk Assessment Guideline
  - BCP and DR Plan

- All publicly available documents including
  - SOC 3 Report
  - CSA CAIQ - STAR Level 1 Assessment
  - Security Whitepaper
  - IS FAQs Document
- And more…

Certinia may add to the profile more documents, reports, and certifications in the future as appropriate. The Full Whistic Security Profile is the only location that Certinia securely shares all of its security documents.

To continue your security evaluation, we'd be happy to share the Full Whistic Security Profile with you if you wish to access and download resources such as our SOC 1, SOC 2, and latest Penetration Test. Please contact your account executive to request access to our Full Profile. All you will need to do to access the profile is create an account.

Data Privacy Resources

Certinia is committed to complying with privacy and data protection laws in the countries in which it operates. At Certinia nothing is more important than the success of our customers and the protection of our customers' data.

Certinia has produced a Guide to the GDPR to help our customers and prospects understand Certinia's response to this important reform of data protection law in Europe.

Additional information about data privacy can be found on our website, inclusive of our:

- Privacy Statement
- Privacy FAQ
- Guide to GDPR
- Data Processing Addendum
- Data Protection Impact Assessment Information Sheet
- And more…

If you have any questions about privacy or our Privacy Statement please direct them to privacy@certinia.com.

Link: https://certinia.com/privacy/