certinia

Certinia Information Security

Frequently Asked Questions

(FAQ)

Effective Date:

May 17, 2024

Information Security Department

Certinia

Table Of Contents

Introduction and Scope

Certinia provides enterprise cloud applications including Enterprise Resource Planning suite of services which comprises of Accounting, Revenue Recognition, Billing Central, Order Procurement and Inventory (OPI), Financial Planning and Analysis, and Reporting and Analytics; and Professional Services Organization Services ("PS Cloud") and the Customer Success Organization Services ("CS Cloud") including PSA, Customer Success Operations (CS Ops) Cloud, and Services CPQ (all collectively referred to as Certinia Applications).

Certinia Applications are built on the Salesforce platform, a cloud computing platform provided by Salesforce. Certinia serves its clients (or "user entities") from headquarters in San Jose, California, USA; with EMEA headquarters in Harrogate, UK (also covers the Asia Pacific region). Founded in 2009, Certinia is backed by Salesforce, Technology Crossover Ventures, Unit4 and Advent International.

The purpose of this document is to provide answers to many of the most frequently asked questions. This should give an extensive overview of the security of Certinia products and services, as well as provide some insights as to how Certinia meets its compliance obligations in various areas. The scope of this document covers Certinia's ERP Cloud, PSA Cloud, and CS Cloud products and services.

Architecture and Data Flow Overview

1. Describe the Certinia product architecture.

    a. Certinia applications were developed on Salesforce, an industry-leading and mature platform for cloud applications provided by Salesforce. Certinia applications are listed on AppExchange (Salesforce cloud applications marketplace) and use the Salesforce platform as the underlying technology, which includes tools for

development, reporting, workflow authorizations, dashboards, social media (Chatter) and integration. All AppExchange applications go through a qualitative and quantitative review process to ensure applications meet a set of security standards and best practices. By leveraging an industry-leading cloud platform for business applications, Certinia applications and our customers' data benefit from a variety of security features and controls in such areas as user management, access control, disaster recovery, backups, physical and network security. As a result, Certinia applications satisfy our customers' most stringent data security requirements, and comply with major security, privacy and data protection laws and standards globally.

2. Public or Private Cloud? Single-tenant or Multi-tenant?

    a. Salesforce provides a Public, Multi-tenant environment. Certinia only provides applications, no infrastructure. Certinia products and services are operated in Salesforce's multitenant architecture that is designed to segregate and restrict Customer Data access based on business needs. The architecture provides an effective logical data separation for different customers via customer-specific "Organization IDs" and allows the use of customer and user role-based access privileges.

3. Where is Customer Data stored? Where geographically is Customer Data stored?

    a. All Customer Data resides solely on the Customer's instance of Salesforce. 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. No Customer Data is stored in the Certinia organization. Since we are 100% natively deployed on the Salesforce platform, Salesforce provides the data centers. Salesforce also provides all of the physical security to protect customer data as a result. Please refer to the Salesforce SOC 2 report for more information.

    In general, Customer Data is stored in data centers in the region from which a customer subscribes to the Covered Services; however, customers can request at the time of sign-up to be hosted in a different region. For customers based in the

Americas, Salesforce stores Customer Data in its data centers located in the United States. For customers based in Europe, the Middle East, and Africa (EMEA), Salesforce stores Customer Data in its data centers located in Europe. For customers based in the Asia Pacific (APAC) region, including Japan and Australia, Salesforce stores Customer Data in its data centers in Japan.

4. Does the Certinia organization store Customer Data?

    a. No. Certinia does not store any data the Customer enters into our products. All data entered by the Customer into Certinia applications resides on the Customer's instance of Salesforce.

5. What cloud platform(s) do the Certinia products/services utilize?

    a. The Salesforce platform is required to use the Certinia applications.

6. Does Certinia have a data center?

    a. No. We do not have a data center. Certinia only provides applications; Salesforce provides the infrastructure. All Customer Data entered into Certinia applications reside on the Customer's Salesforce instance. Customer Data is not stored in Certinia organization systems.

7. Describe the data flow of Customer Data.

    a. Certinia is an application native to the Salesforce platform. All data entered by the Customer into Certinia ("Customer Data"), and the Certinia managed package (i.e. application) itself, will reside in a Salesforce instance (Org) either previously purchased by Customer from Salesforce or provided by Certinia at the time of purchase. In other words, all data entered in the Certinia applications is directly stored on the Salesforce platform. Note: Certinia will not have access to Customer Data without customer's permission. All access is managed, monitored and terminated by the Customer. Customers are responsible for managing their own customer data, including access controls.

***Note: For visual guides to the architecture and data flow of Certinia products and services, please refer to our Security Whitepaper as well as the diagrams presented in the last question of this section.

8. What interfaces or integrations are required?

    a. There are no interfaces or integrations required for our products. Salesforce is required as it is the infrastructure platform that our applications run on.

    Certinia has several integrations that are currently available. Please visit our website for a current list of the growing number of supported integrations: https://certinia.com/support-services/integrations/

    Any 3rd party integrations with Salesforce are determined by the customer and are the responsibility of the customer.

9. Will Certinia personnel have access to Customer Data?

    a. No. Given that the Certinia applications reside and store data on the Customer's instance of Salesforce, the Customer has control over who has access to Customer Data.

    Certinia is an application native to the Salesforce platform. All data entered by the Customer into Certinia ("Customer Data"), and the Certinia managed package (i.e. application) itself, will reside in a Salesforce instance (Org) either previously purchased by Customer from Salesforce or provided by Certinia at the time of purchase. Note: Certinia will not have access to Customer Data without customer's permission. However, if Customer purchases maintenance support or implementation services, then Certinia Customer Support or Professional Services may have access to In-Scope Information as needed to diagnose and resolve support cases. In this case, Customer is responsible for provisioning roles, permissions and grant access to Certinia staff in order to complete the services required. Customers would thus have to provision access to Certinia customer support using the Salesforce Platform "Login As" process. All access is managed,

monitored and terminated by the Customer. This is the only scenario in which Certinia will have access to data you store in our products.

Customers are responsible for managing their own customer data, including access controls. Customer data is processed and stored on the Salesforce platform. Please refer to the section **Access and Authentication** for more information regarding access controls.

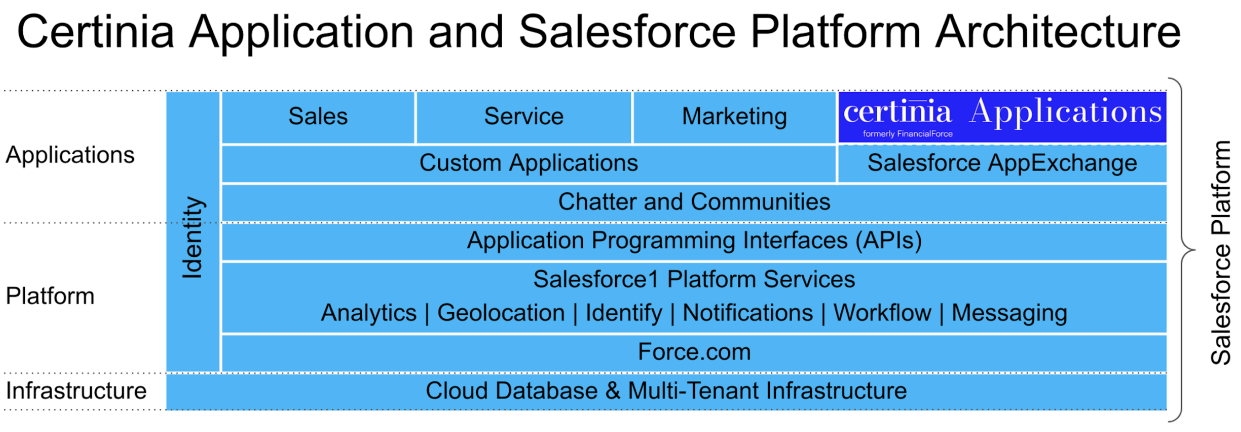
10. Is Customer Data logically and/or physically segregated?

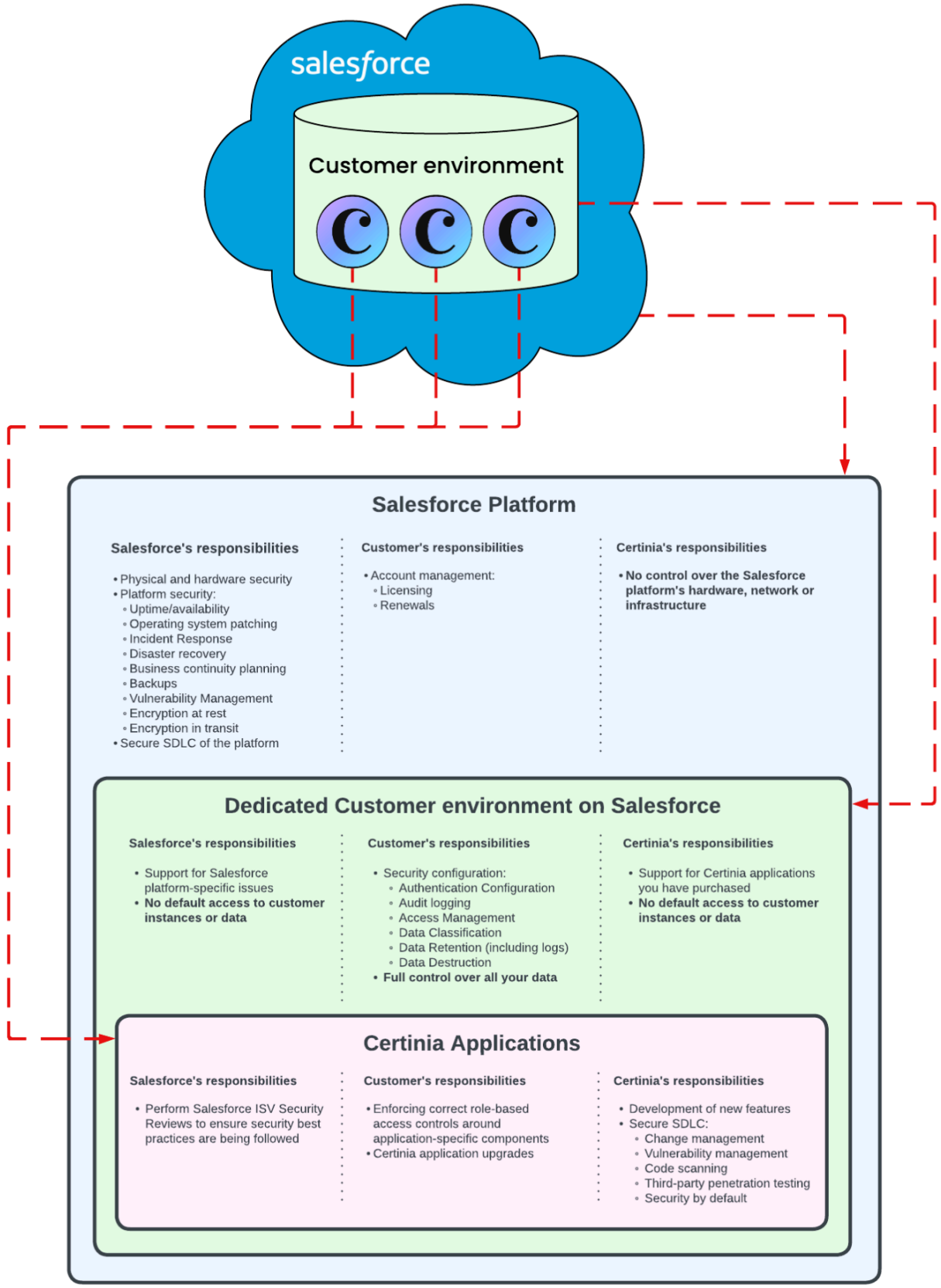
    a. Yes, Certinia applications are operated in Salesforce's multitenant architecture that is designed to segregate and restrict Customer Data access based on business needs. The architecture provides an effective logical data separation for different customers via customer-specific "Organization IDs" and allows the use of customer and user role-based access privileges.

11. Is data encrypted at rest? Is data encrypted in transit?

    a. Yes, the Salesforce platform has data encryption capabilities both at rest and in transit. Please refer to the section **Backups and Encryption** for more detailed information regarding encryption of data at rest and in transit.

12. Below are two diagrams illustrating the relationship of Certinia products/services.




salesforce
Customer environment
Salesforce Platform
Salesforce's responsibilities
• Physical and hardware security
• Platform security:
◦ Uptime/availability
◦ Operating system patching
◦ Incident Response
◦ Disaster recovery
◦ Business continuity planning
◦ Backups
◦ Vulnerability Management
◦ Encryption at rest
◦ Encryption in transit
• Secure SDLC of the platform
Customer's responsibilities
• Account management:
◦ Licensing
◦ Renewals
Certinia's responsibilities
• No control over the Salesforce platform's hardware, network or infrastructure
Dedicated Customer environment on Salesforce
Salesforce's responsibilities
• Support for Salesforce platform-specific issues
• No default access to customer instances or data
Customer's responsibilities
• Security configuration:
◦ Authentication Configuration
◦ Audit logging
◦ Access Management
◦ Data Classification
◦ Data Retention (including logs)
◦ Data Destruction
• Full control over all your data
Certinia's responsibilities
• Support for Certinia applications you have purchased
• No default access to customer instances or data
Certinia Applications
Salesforce's responsibilities
• Perform Salesforce ISV Security Reviews to ensure security best practices are being followed
Customer's responsibilities
• Enforcing correct role-based access controls around application-specific components
• Certinia application upgrades
Certinia's responsibilities
• Development of new features
• Secure SDLC:
◦ Change management
◦ Vulnerability management
◦ Code scanning
◦ Third-party penetration testing
◦ Security by default

For more information, please refer to Salesforce's guide on platform architecture.

Please also refer to our **Salesforce Application Architecture Data Flow** document also available on our Whistic Profile.

Major Compliance Reports and Frameworks

Below is a table outlining the various third-party attestations, certifications, frameworks, and self-assessments that Certinia has, does not have, or is not applicable. All Certinia security documents are made available through our Full Whistic Profile but not always through our Public Whistic Profile. As such, guidance is provided for each line item in the table accordingly.

Attestation, Certification, or Framework	Answer	Notes/Comment
SOC 1	Yes	This is only available through our Full Whistic Profile. Please contact your account executive or sales representative to request access to our Full Whistic Profile.
SOC 2	Yes	This is only available through our Full Whistic Profile. Please contact your account executive or sales representative to request access to our Full Whistic Profile.
SOC 3	Yes	Our SOC 3 report is available both on our Trust website as well as through our Public Whistic Profile.
ISO 27001	No	Certinia is not ISO 27001 certified. Salesforce is ISO 27001 certified and provides the network, infrastructure, and platform related controls as part of the shared security responsibilities model. All Customer Data resides on the Customer's instance of Salesforce. For more information on the architecture and data flow for Certinia applications, please refer to the section **Architecture and Data Flow Overview**.
PCI	Not Applicable	Certinia products and services do not fall within the scope of PCI compliance requirements.

FedRAMP	Not Applicable	Certinia provides only applications; Salesforce provides the infrastructure. As Certinia does not provide the infrastructure, Certinia cannot be fully considered for FedRAMP compliance. Certinia is aligned to a subset of FedRAMP controls, but Certinia cannot be fully FedRAMP compliant due to the nature of the architecture. Certinia engages with a third-party assessor which issues an annual compliance whitepaper that validates Certinia's alignment with the subset of applicable FedRAMP controls. This FedRAMP compliance whitepaper can be made available upon request. Additionally, please refer to the section **Architecture and Data Flow Overview** for more clarity on the architecture and data flow of Certinia applications.
CSA CAIQ	Yes	This is available both on our Public Whistic Profile and through the CSA website: https://cloudsecurityalliance.org/star/registry/financialforce/services/financialforce/
VSA	Yes	This is available on our Full Whistic Profile.
SIG Lite	Yes	This is available on our Public Whistic Profile.

Network and Infrastructure Security

1. What is the shared security responsibilities model? Why is this important for understanding the security of Certinia applications?

    a. Moving business processes and applications to the cloud creates a shared responsibility model between our customers, Certinia and Salesforce. This shared model maximizes efficiency and flexibility while maintaining a high level of security. Certinia manages and controls its applications and related services. This includes change management, incident management, product updates and patch management related to the Certinia applications. Salesforce operates, manages and controls the components from the API level down to the host operating system, underlying databases and physical security of data centers in which the services operate. For details on Salesforce security, see trust.salesforce.com and search "security" on help.salesforce.com.

Customers are responsible for user access and authorization, control and backup of data uploaded to the Certinia applications, as well as configuration of the underlying Salesforce platform in accordance with their requirements. Customers can also enhance the security of their Certinia implementation and address security and compliance requirements by leveraging security features of the Salesforce platform such as data encryption, IP-range restrictions, two-factor authentication, strong passwords and enforced periodic password changes. Certinia recognizes that many companies are subject to regulations and standards governing security and handling of information, and therefore maintains a security program that covers policies, practices, people and technology. However, to use Certinia applications securely, customers must apply sound security practices to their configuration and any customization and integration of Certinia and the underlying Salesforce platform, including customers' design and implementation of related business processes.

Please refer to the section **Architecture and Data Flow Overview** for more information.

2. Where can I find more information about network and infrastructure security given Certinia only provides applications?

    a. Certinia provides only applications; Salesforce provides the infrastructure. All Customer Data entered into Certinia apps reside directly on the Customer's instance of Salesforce. As such, please refer to Salesforce's SOC 2 Type II report and/or other compliance documentation available through their website.

3. Is there an IDS deployed to protect the network? What about WAF?

    a. Yes, Salesforce provides IDS as part of the data center implementation.

    No, Salesforce does not have a WAF deployed.

    Certinia only provides applications; Salesforce provides the infrastructure. For more information and clarification of this distinction in the architecture, please refer to the section **Architecture and Data Flow Overview**.

4. Is IP Whitelisting available to restrict network access?

    a. Yes, IP whitelisting is available. Customers can control login access at the user level by specifying a range of allowed IP addresses on a user's profile. When Customer defines IP address restrictions for a profile, a login from any other IP address is denied.

Backups and Encryption

1. How is customer data backed up?

    a. A combination of near real-time data replication and data backups are utilized to protect Customer Data. Data centers are configured in pairs, so primary production infrastructure and production data are fully replicated to secondary sites. Customers are also encouraged to conduct their own backup by leveraging the native Salesforce CSV data export feature or commercial solutions.

2. How is customer data encrypted at rest?

    a. Encryption capabilities at rest are leveraged through Salesforce. Certinia only provides applications; Salesforce provides the infrastructure. All Customer Data entered into Certinia apps directly reside on the Customer's instance of Salesforce.

    By default, Hyperforce customers benefit from *volume-level* encryption for data at rest. Volume-level encryption protects all the data on a disk with one encryption key, which Salesforce owns and manages.

    Additional to volume-level encryption, *Platform Encryption* is a paid Salesforce platform feature which allows the Customer to encrypt certain standard fields, as well as custom fields, and bears less limitations than Classic Encryption over what custom fields you can encrypt. Platform Encryption uses Advanced Encryption Standard (AES) with 256-bit keys with CBC mode, and a static initialization vector (IV), which is a hash of the entity ID, field ID, and key ID, making it unique to each

customer and field per org. It comes in 2 forms: Probabilistic and Deterministic Platform Encryption.

Salesforce is working on tenant-level encryption (TLE) which, at the time of writing, is not in GA.

3. How is customer data encrypted in transit?

    a. Encryption capabilities for data in transit are leveraged through Salesforce. Certinia only provides applications; Salesforce provides the infrastructure. All Customer Data entered into Certinia apps directly reside on the Customer's instance of Salesforce. The Salesforce platform uses industry-standard encryption to protect customer data and communications in transit between a customer's network and the Salesforce data centers, including 128-bit TLS Certificates and 2048-bit RSA public keys at a minimum.

Business Continuity and Disaster Recovery

1. What is the shared security responsibilities model? Why is it critical for understanding the security of Certinia products?

    a. Moving business processes and applications to the cloud creates a shared responsibility model between our customers, Certinia and Salesforce. This shared model maximizes efficiency and flexibility while maintaining a high level of security. Certinia manages and controls its applications and related services. This includes change management, incident management, product updates and patch management related to the Certinia applications. Salesforce operates, manages and controls the components from the API level down to the host operating system, underlying databases and physical security of data centers in which the services operate. For details on Salesforce security, see trust.salesforce.com and search "security" on help.salesforce.com.

Customers are responsible for user access and authorization, control and backup of data uploaded to the Certinia applications, as well as configuration of the underlying Salesforce platform in accordance with their requirements. Customers can also enhance the security of their Certinia implementation and address security and compliance requirements by leveraging security features of the Salesforce platform such as data encryption, IP-range restrictions, two-factor authentication, strong passwords and enforced periodic password changes. Certinia recognizes that many companies are subject to regulations and standards governing security and handling of information, and therefore maintains a security program that covers policies, practices, people and technology. However, to use Certinia applications securely, customers must apply sound security practices to their configuration and any customization and integration of Certinia and the underlying Salesforce platform, including customers' design and implementation of related business processes.

Please refer to the section **Architecture and Data Flow Overview** for more information.

2. Does Certinia have a Business Continuity Plan? How often is it tested?

    a. Yes, Certinia has a BC Plan that is tested at least annually. Salesforce also has Business Continuity controls and a BCP that are directly relevant to the scope of Customer Data. All Customer Data resides on the Customer's instance of Salesforce. Certinia only provides applications; Salesforce provides the infrastructure. For more detailed information regarding BCP, please refer to Salesforce's compliance documents.

3. Does Certinia have a Disaster Recovery Plan/Procedure? How often is it tested?

    a. Yes, Certinia has a DR Plan that is tested at least annually. Salesforce also has Disaster Recovery controls and a DR Plan that are directly relevant to the scope of Customer Data. All Customer Data resides on the Customer's instance of Salesforce. Certinia only provides applications; Salesforce provides the infrastructure. For more information regarding BCP, please refer to Salesforce's compliance documents.

4. What are the recovery and uptime SLAs?

    a. Because Salesforce provides the infrastructure and all Customer Data entered into Certinia applications resides directly on the Customer's Salesforce instance, recovery and uptime SLAs are passed down from Salesforce. Salesforce is committed to a 12 hour RTO and 4 hour RPO.

    The Salesforce Services' disaster recovery plans currently have the following target recovery objectives: (a) restoration of the Salesforce Service within 12 hours (RTO) after Salesforce's declaration of a disaster; and (b) maximum Customer Data loss of 4 hours (RPO); excluding, however, a disaster or multiple disasters causing the compromise of both data centers at the same time, and excluding development and test bed environments, such as the Sandbox service.

Access and Authentication

1. Who controls authentication means, methods, and/or requirements to Certinia products and services?

    a. All authentication and access to Certinia applications is through Salesforce. Customers have control over authentication and access configurations and controls for their own Salesforce instance. Certinia does not manage this on behalf of the Customer.

2. What methods of authentication are available?

    a. All authentication is through the Salesforce platform. Authentication methods to Salesforce include username + password, SSO, and Multi-Factor Authentication. All methods can be customized to meet the Customer's security requirements from the Salesforce platform.

3. What are the password requirements?

a. Customers can customize password and other configurations for their own Salesforce instance to meet their security requirements. Certinia does not manage this on behalf of the Customer.

4. Is SSO supported?

    a. Yes, Salesforce fully supports SSO capabilities. Certinia does not manage configurations for the Customer's Salesforce instance.

5. Is MFA supported?

    a. Yes, Salesforce requires MFA. Customers can configure MFA to meet their needs according to their environment. Certinia does not manage this on behalf of the Customer.

6. Who manages access to Certinia products and services?

    a. Customers are responsible for managing access for their own Salesforce instance. Certinia does not manage access to the Customer's Salesforce instance on behalf of the Customer. As stated previously, all access to the Certinia applications is through Salesforce.

7. Does Certinia have access to Customer Data or the Customer environment?

    a. No. By default, Certinia does not have access to the Customer's Salesforce instance. Thus, by default, Certinia does not have access to the Customer's implementation of Certinia applications on Salesforce. Certinia Customer Support personnel may require access to In-Scope Information as needed to diagnose and resolve support cases. Any such access must be authorized by the Customer on a case-by-case basis using the Salesforce Platform "Login As" process. This is the only scenario in which Certinia would have access to Customer Data entered in Certinia applications and stored on the Customer's Salesforce instance.

8. Is role-based access utilized? Segregation of duties?

a. Yes, Customers are responsible for configuring role-based access and segregation of duties for their Salesforce instance. Certinia delivers functionality-centric, out of the box, role-based permissions for major Certinia products which can be customized to meet the business needs of each Customer. Certinia does not manage role customization or access provisioning on behalf of the Customer.

9. Are controls for access provisioning, de-provisioning, and periodic review implemented?

    a. Yes, Customer is responsible for implementing access management controls such as provisioning, de-provisioning, and regular periodic review of access for their own Salesforce instance. Certinia does not manage access controls in the Customer's Salesforce instance on behalf of the Customer.

10. Does Certinia require access to servers, databases, or any other assets supporting the underlying infrastructure?

    a. No. Certinia applications are 100% native to the Salesforce platform. Certinia applications cannot function without Salesforce's platform infrastructure. Certinia only provides applications; Salesforce provides the infrastructure. As stated previously, Certinia Customer Support personnel may require access to the Customer's Salesforce instance as needed to diagnose and resolve support cases. Any such access must be authorized by the Customer on a case-by-case basis using the Salesforce Platform "Login As" process. This is the only scenario in which Certinia would have access to Customer Data entered in Certinia applications and stored on the Customer's Salesforce instance.

11. Is remote access required?

    a. No. All access to Certinia applications is through normal Salesforce access over a secure browser using TLS 1.2. As stated above, only one scenario exists where Certinia may require access to the Customer's instance of Salesforce - that being for diagnosis and resolution of customer support cases as needed, and access is provisioned at the sole discretion of the Customer.

Incident Management

1. Does Certinia have an incident response/management procedure?

    a. Yes, Certinia maintains security incident management policies and procedures, which include prompt notification of customers in the event Certinia becomes aware of an actual or reasonably suspected unauthorized use or disclosure of customer data.

2. How does Salesforce factor into the incident response process?

    a. All Customer Data resides on the Customer's instance of Salesforce. The data that the Customer enters into our applications stays directly on the Customer's instance of Salesforce - Certinia organization systems do not store Customer Data. As such, Certinia partners closely with Salesforce to ensure timely, appropriate, and effective security incident management.

3. How are notifications for incidents such as data breaches handled?

    a. Certinia coordinates closely with Salesforce to ensure that Customers are notified promptly without undue delay when Certinia becomes aware of an actual or reasonably suspected unauthorized use or disclosure of customer data. Certinia shall notify 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 Certinia or its Sub-processors of which Certinia becomes aware. Notifications will be sent to a customer email address on file. Similarly, Customers may contact security@certinia.com for more information relating to any security issues or matters that need to be addressed.

4. Does the security team provide updates regarding potential impacts of major vulnerabilities?

    a. Certinia additionally monitors its organization systems closely and provides security advisories detailing as to whether Certinia systems have been impacted by major

vulnerabilities. Such news and updates can be found on our website: https://certinia.com/trust/security-advisories/

For Salesforce: https://security.salesforce.com/security-advisories/

Change Management and Product Security

1. Describe the security measures included in Certinia's software development lifecycle.

    a. Certinia follows fully documented change management procedures for all aspects of its software lifecycle, including application development, release management, service management and enhancement.

    Certinia's software development lifecycle incorporates a number of security measures, including:

        i. Code reviews designed to ensure adherence to Certinia development standards.

        ii. Software security testing and code scanning to identify and address security vulnerabilities.

        iii. Release reviews and approvals designed to ensure product releases comply with internal process requirements.

        iv. Vulnerability testing and remediation for infrastructure and tools supporting our source code management platform.

        v. Development and changes to production application systems are authorized, tested, approved and documented.

2. Does Certinia have fully documented change management procedures? What's included as part of established governance?

    a. Certinia follows fully documented change management procedures for all aspects of its software lifecycle, including application development, release management, service management and enhancement.

More information can be found in the Certinia SOC 3 and Security Whitepaper.

3. What is the Salesforce AppExchange? What is the relevant Security Review?

    a. Certinia applications were developed on Salesforce, an industry-leading and mature platform for cloud applications provided by Salesforce. Certinia applications are listed on AppExchange (Salesforce cloud applications marketplace) and use the Salesforce platform as the underlying technology, which includes tools for development, reporting, workflow authorizations, dashboards, social media (Chatter) and integration. All AppExchange applications go through a qualitative and quantitative review process to ensure applications meet a set of security standards and best practices. By leveraging an industry-leading cloud platform for business applications, Certinia applications and our customers' data benefit from a variety of security features and controls in such areas as user management, access control, disaster recovery, backups, physical and network security. As a result, Certinia applications satisfy our customers' most stringent data security requirements, and comply with major security, privacy and data protection laws and standards globally.

    b. Certinia applications are submitted to Salesforce as part of the AppExchange Security Review process. Salesforce provides the AppExchange Security Review program to assess the security posture of ISV applications published on the AppExchange against industry best practices for security.

4. What are some of the application controls provided to ensure the security, availability, integrity, confidentiality, completeness, and accuracy of data and transactions?

    a. Certinia provides rigorous application controls that ensure your financial transactions have been correctly validated and reviewed prior to posting, have comprehensive audit trails and cannot subsequently be modified via "back door" manipulation of object data.

    These application controls include:

i. Comprehensive audit trails for transactions, master data modifications and security setup changes.

ii. Multi-level approval processes for transactions and master file data changes

iii. Segregation of duties

iv. Highly granular control of company, object, record and field level access by role

More detailed information can be obtained from our Security Whitepaper, SOC 1 report, and SOC 2 report.

IS Governance, Risk, and Compliance

Governance

1. Describe Certinia's organization structure around information security.

    a. Everyone at Certinia, from the research and development staff to the executive team, is committed to security excellence. The company's Head of Information Security coordinates a cross-functional team of experts focused on security-related activities. The Head of Information Security leads the Information Security department which is segregated from IT to ensure appropriate independence. Certinia also has a Senior Vice President and General Counsel with responsibility for compliance with global privacy laws. All employees receive regular information security awareness training that covers key security threats and risks and employee obligations to protect the security, confidentiality and privacy of customer and company data.

2. Does Certinia have an information security policy? Additional supporting policies?

    a. Certinia has a dedicated Security and Trust function that coordinates security policy, program and verification efforts, to ensure that customer and company

information assets are adequately protected. Our Information Security Program includes identifying, evaluating and reporting on security risks, compliance with security and privacy regulations and commitments, threat and vulnerability management, and security incident management and response. Certinia has an Information Security Policy and Standards framework based on ISO 27001/27002 that describe standards, best-practice guidelines and approaches required to protect customer data and corporate assets (including people, information and infrastructure).

Certinia has numerous supporting policies that establish requirements and meet compliance objectives. Further details can be found in our SOC 1 and SOC 2 reports through our Full Whistic Profile.

3. Does Certinia have an Information Security Charter?
    a. Yes, Certinia has established an IS Charter.

Risk

1. Does Certinia have a risk management policy/procedure?
    a. Yes, Certinia has established and implemented a risk management policy.
2. Does Certinia assess the risks of its critical third-party suppliers relevant to the delivery of its products?
    a. Yes, at least annually.
3. Does Certinia conduct background checks for all personnel?
    a. Yes, background checks are conducted subject to local laws and regulations.
4. Does Certinia conduct cyber security awareness training?
    a. Yes, training is required at onboarding and at least annually thereafter.

5. Are contracted third-party personnel subject to security review and Certinia onboarding processes?
    a. Yes.
6. Are all personnel subject to acknowledgment of the company's Acceptable Use Policy?
    a. Yes, at least annually with training.

Compliance

1. Who oversees data privacy compliance at Certinia?
    a. Certinia has dedicated Legal and Privacy functions including a Privacy Officer who directly oversee data privacy compliance. More information can be found here: https://www.certinia.com/privacy/
2. Where to find more information on data privacy compliance?
    a. https://www.certinia.com/privacy/
3. Additional resources?
    a. Please see our Privacy FAQ for a primer on data privacy compliance at Certinia. https://www.certinia.com/privacy/financialforce-privacy-faq/

For more information regarding the relevant attestation reports, assessments, certifications, and security frameworks applicable to Certinia, please refer to the section **Major Compliance Reports and Frameworks.**