

# FinancialForce Information Security Frequently Asked Questions (FAQ)

**Effective Date:**  
**December 23, 2022**

Information Security

FinancialForce

## Table Of Contents

Introduction and Scope	3
Architecture and Data Flow Overview	3
Major Compliance Reports and Frameworks	7
Network and Infrastructure Security	8
Backups and Encryption	9
Business Continuity and Disaster Recovery	10
Access and Authentication	12
Incident Management	14
Change Management and Product Security	15
Information Security Governance, Risk, and Compliance	16
Governance	16
Risk	17
Compliance	18

## Introduction and Scope

FinancialForce.com provides enterprise cloud applications including Financial Management, Professional Services Automation (PSA), and Human Capital Management (HCM) (collectively referred to as FinancialForce Applications). FinancialForce applications are built on the Force.com platform, a cloud computing platform provided by Salesforce. FinancialForce serves its clients (or “user entities”) from headquarters in San Francisco, California, USA, with EMEA headquarters in Harrogate, UK (also covers the Asia Pacific region). Founded in 2009 and headquartered in San Francisco, FinancialForce 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 FinancialForce products and services, as well as provide some insights as to how FinancialForce meets its compliance obligations in various areas. The scope of this document covers FinancialForce’s ERP Cloud, PSA Cloud, and CS Cloud products and services.

## Architecture and Data Flow Overview

1. Describe the FinancialForce product architecture.
  - a. FinancialForce applications were developed on Force.com, an industry-leading and mature platform for cloud applications provided by Salesforce. FinancialForce applications are listed on AppExchange (Salesforce cloud applications marketplace) and use the Force.com cloud 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, FinancialForce 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, FinancialForce 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. FinancialForce only provides applications, no infrastructure. FinancialForce 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 are Customer Data stored? Where geographically are 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 FinancialForce applications reside on the Salesforce cloud platform owned, operated and managed by Salesforce. No Customer Data is stored in the FinancialForce 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 FinancialForce organization store Customer Data?

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

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

- a. The Salesforce platform is required to use the FinancialForce applications.

6. Does FinancialForce have a data center?

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

7. Describe the data flow of Customer Data.

- a. FinancialForce is an application native to the Salesforce platform. All data entered by the Customer into FinancialForce ("Customer Data"), and the FinancialForce managed package

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

\*\*\*Note: For visual guides to the architecture and data flow of FinancialForce 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.

FinancialForce has several integrations that are currently available. Please visit our website for a current list of the growing number of supported integrations:

<https://www.financialforce.com/support-services/integrations/>

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

9. Will FinancialForce personnel have access to Customer Data?

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

To reiterate, FinancialForce is an application native to the Salesforce platform. All data entered by the Customer into FinancialForce ("Customer Data"), and the FinancialForce managed package (i.e. application) itself, will reside in a Salesforce instance (Org) either previously purchased by Customer from Salesforce or provided by FinancialForce at the time of purchase. Note: FinancialForce will not have access to Customer Data without customer's permission. However, if Customer purchases maintenance support or implementation services, then FF 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 FinancialForce staff in order to complete the services required. Customer would thus have to provision access to FinancialForce 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 FinancialForce will have access to data you store in our products.

Customer is responsible for managing its 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?

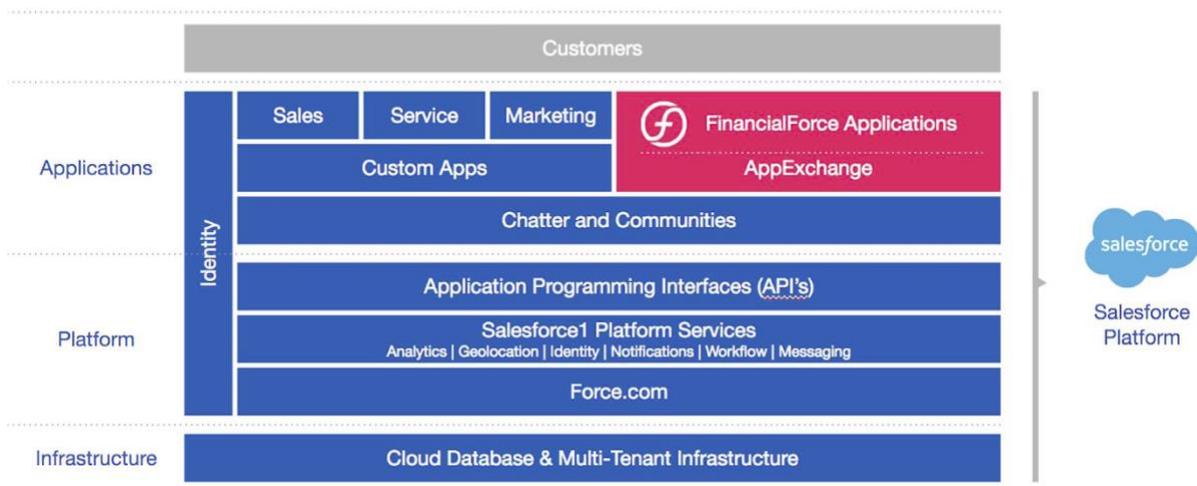
- a. Yes, FinancialForce applications are operated in Salesforce's multitenant architecture that is designed to segregate and restrict Customer Data access based on business needs. The architecture provides an effective logical data separation for different customers via customer-specific "Organization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

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

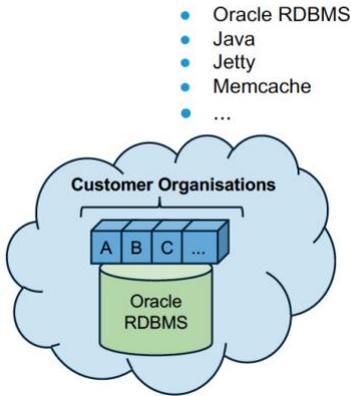
- a. Yes, the Salesforce platform has data encryption capabilities both at rest and in transit. Please refer to the section [Backups and Encryption](#) for more detailed information regarding encryption of data at rest and in transit.

12. Attach a diagram illustrating Customer Data flows for FinancialForce products/services.

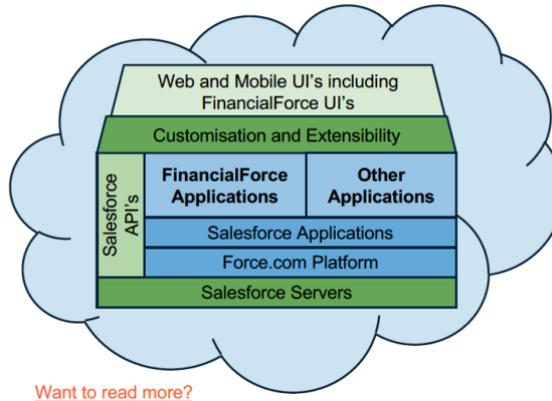
## FinancialForce Application & Salesforce Platform Architecture



### Force.com Under the Hood ...



### FinancialForce builds “Native” Force.com Apps



[Want to read more?](#)

For more information, please refer to Salesforce’s guide on [platform architecture](#).

Please also refer to our **Force.com 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 FinancialForce has, does not have, or is not applicable. All FinancialForce 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	FinancialForce 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 FinancialForce applications, please refer to the section <a href="#">Architecture and Data Flow Overview</a> .
PCI	Not Applicable	FinancialForce products and services do not fall within the scope of PCI compliance requirements.

FedRAMP	Not Applicable	<p>FinancialForce provides only applications; Salesforce provides the infrastructure. As FinancialForce does not provide the infrastructure, FinancialForce cannot be fully considered for FedRAMP compliance.</p> <p>FinancialForce is aligned to a subset of FedRAMP controls, but FinancialForce cannot be fully FedRAMP compliant due to the nature of the architecture. FinancialForce engages with a third-party assessor which issues an annual compliance whitepaper that validates FinancialForce's alignment with the subset of applicable FedRAMP controls. This FedRAMP compliance whitepaper can be made available upon request.</p> <p>Additionally, please refer to the section <a href="#">Architecture and Data Flow Overview</a> for more clarity on the architecture and data flow of FinancialForce applications.</p>
CSA CAIQ	Yes	This is available both on our Public Whistic Profile and through the CSA website: <a href="https://cloudsecurityalliance.org/star/registry/financialforce/services/financialforce/">https://cloudsecurityalliance.org/star/registry/financialforce/services/financialforce/</a>
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 FinancialForce applications?
  - a. Moving business processes and applications to the cloud creates a shared responsibility model between our customers, FinancialForce and Salesforce. This shared model maximizes efficiency and flexibility while maintaining a high level of security. FinancialForce manages and controls its applications and related services. This includes change management, incident management, product updates and patch management related to the FinancialForce 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](https://trust.salesforce.com) and search "security" on [help.salesforce.com](https://help.salesforce.com).

Customers are responsible for user access and authorization, control and backup of data uploaded to the FinancialForce applications, as well as configuration of the underlying Salesforce platform in accordance with their requirements. Customers can also enhance the security their FinancialForce implementation and address security and compliance requirements by leveraging security features of the Force.com platform such as data encryption, IP-range restrictions, two-factor authentication, strong passwords and enforced periodic password changes. FinancialForce 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 FinancialForce applications securely, customers must apply sound security practices to

their configuration and any customization and integration of FinancialForce 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 FinancialForce only provides applications?
  - a. FinancialForce provides only applications; Salesforce provides the infrastructure. All Customer Data entered into FinancialForce 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.  
  
FinancialForce 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. Customer 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. Customer is also encouraged to conduct their own backup by exporting to a .csv file format on a continual basis.
  
2. How is customer data encrypted at rest?

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

Customers must purchase the optional Salesforce Platform Encryption at cost to enable encryption of data at rest. Note: When Platform Encryption is deployed and when using FinancialForce PSA, only Contact Name and Account Name fields can be encrypted within the PSA application.

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.

### 3. How is customer data encrypted in transit?

- a. Encryption capabilities for data in transit are leveraged through Salesforce. FinancialForce only provides applications; Salesforce provides the infrastructure. All Customer Data entered into FinancialForce apps directly reside on the Customer's instance of Salesforce. The Salesforce platform uses industry-accepted encryption products 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 FinancialForce products?
  - a. Moving business processes and applications to the cloud creates a shared responsibility model between our customers, FinancialForce and Salesforce. This shared model maximizes efficiency and flexibility while maintaining a high level of security. FinancialForce manages and controls its applications and related services. This includes change management, incident management, product updates and patch management related to the FinancialForce 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](https://trust.salesforce.com) and search “security” on [help.salesforce.com](https://help.salesforce.com).

Customers are responsible for user access and authorization, control and backup of data uploaded to the FinancialForce applications, as well as configuration of the underlying Salesforce platform in accordance with their requirements. Customers can also enhance the security their FinancialForce implementation and address security and compliance requirements by leveraging security features of the Force.com platform such as data encryption, IP-range restrictions, two-factor authentication, strong passwords and enforced periodic password changes. FinancialForce 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 FinancialForce applications securely, customers must apply sound security practices to their configuration and any customization and integration of FinancialForce 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 FinancialForce have a Business Continuity Plan? How often is it tested?
  - a. Yes, FinancialForce 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. FinancialForce only provides applications; Salesforce provides the infrastructure. For more detailed information regarding BCP, please refer to Salesforce's compliance documents.
3. Does FinancialForce have a Disaster Recovery Plan/Procedure? How often is it tested?
  - a. Yes, FinancialForce 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. FinancialForce 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 FinancialForce applications resides directly on the Customer's Salesforce instance, recovery and uptime SLAs are passed down from Salesforce. Salesforce is committed to a 99% uptime SLA, and 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 FinancialForce products and services?
  - a. All authentication and access to FinancialForce applications is through Salesforce. Customer has control over authentication and access configurations and controls for their own Salesforce instance. FinancialForce 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. Customer can customize password and other configurations for their own Salesforce instance to meet their security requirements. FinancialForce does not manage this on behalf of the Customer.
4. Is SSO supported?
  - a. Yes, Salesforce fully supports SSO capabilities. FinancialForce does not manage configurations for the Customer's Salesforce instance.
5. Is MFA supported?
  - a. Yes, Salesforce requires MFA. Customer can configure MFA to meet their needs according to their environment. FinancialForce does not manage this on behalf of the Customer.
6. Who manages access to FinancialForce products and services?

- a. Customer is responsible for managing access for their own Salesforce instance. FinancialForce does not manage access to the Customer's Salesforce instance on behalf of the Customer. As stated previously, all access to the FinancialForce applications is through Salesforce.
7. Does FinancialForce have access to Customer Data or the Customer environment?
    - a. No, by default, FinancialForce does not have access to the Customer's Salesforce instance. Thus, by default, FinancialForce does not have access to the Customer's implementation of FinancialForce applications on Salesforce. FinancialForce 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 FinancialForce would have access to Customer Data entered in FinancialForce applications and stored on the Customer's Salesforce instance.
  8. Is role-based access utilized? Segregation of duties?
    - a. Yes, Customer is responsible for configuring role-based access and segregation of duties for their Salesforce instance. FinancialForce does not manage this 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. FinancialForce does not manage access controls in the Customer's Salesforce instance on behalf of the Customer.
  10. Does FinancialForce require access to servers, databases, or any other assets supporting the underlying infrastructure?
    - a. No. FinancialForce applications are 100% native to the Salesforce force.com platform. FinancialForce applications cannot function without Salesforce's platform infrastructure. FinancialForce only provides applications; Salesforce provides the infrastructure. As stated previously, FinancialForce 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 FinancialForce would have access to Customer Data entered in FinancialForce applications and stored on the Customer's Salesforce instance.
  11. Is remote access required?

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

## Incident Management

1. Does FinancialForce have an incident response/management procedure?
  - a. Yes, FinancialForce maintains security incident management policies and procedures, which include prompt notification of customers in the event FinancialForce becomes aware of an actual or reasonably suspected unauthorized use or disclosure of customer data.
2. How does Salesforce factor in to 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 - FinancialForce organization systems do not store Customer Data. As such, FinancialForce 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. FinancialForce coordinates closely with Salesforce to ensure that Customers are notified promptly without undue delay when FinancialForce becomes aware of an actual or reasonably suspected unauthorized use or disclosure of customer data. FF 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 FF or its Sub-processors of which FF becomes aware. Notifications will be sent to a customer email address on file. Similarly, Customer may contact [security@financialforce.com](mailto:security@financialforce.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. FinancialForce additionally monitors its organization systems closely and provides security advisories detailing as to whether FinancialForce systems have been impacted by major vulnerabilities. Such news and updates can be found on our website: <https://www.financialforce.com/legal-privacy-trust/trust/security-advisories/>  
  
For Salesforce: <https://security.salesforce.com/security-advisories/>

## Change Management and Product Security

1. Describe the security measures included in FinancialForce's software development lifecycle.
  - a. FinancialForce follows fully documented change management procedures for all aspects of its software lifecycle, including application development, release management, service management and enhancement.

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

- i. Code reviews designed to ensure adherence to FinancialForce 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 FinancialForce have fully documented change management procedures? What's included as part of established governance?
  - a. FinancialForce 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 FinancialForce SOC 3 and Security Whitepaper.

3. What is the Salesforce AppExchange? What is the relevant Security Review?
  - a. FinancialForce applications were developed on Force.com, an industry-leading and mature platform for cloud applications provided by Salesforce. FinancialForce applications are listed on AppExchange (Salesforce cloud applications marketplace) and use the Force.com cloud 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, FinancialForce 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, FinancialForce applications satisfy our customers' most stringent data security requirements, and comply with major security, privacy and data protection laws and standards globally.

- b. FinancialForce 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. FinancialForce 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.

## Information Security Governance, Risk, and Compliance

### Governance

1. Describe FinancialForce's organization structure around information security.
  - a. Everyone at FinancialForce, from the research and development staff to the executive team, is committed to security excellence. The company's Chief Information Security Officer (CISO) coordinates a cross-functional team of experts focused on security-related activities. The CISO

leads the Information Security department which is segregated from IT to ensure appropriate independence. FinancialForce 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 FinancialForce have an information security policy? Additional supporting policies?
  - a. FinancialForce 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. FinancialForce 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).  
  
FinancialForce 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 FinancialForce have an Information Security Charter?
  - a. Yes, FinancialForce has established an IS Charter.

## **Risk**

1. Does FinancialForce have a risk management policy/procedure?
  - a. Yes, FinancialForce has established and implemented a risk management policy.
2. Does FinancialForce assess the risks of its critical third-party suppliers relevant to the delivery of its products?
  - a. Yes, at least annually.
3. Does FinancialForce conduct background checks for all personnel?
  - a. Yes, background checks are conducted subject to local laws and regulations.
4. Does FinancialForce 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 FinancialForce 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 FinancialForce?
- a. FinancialForce has dedicated Legal and Privacy functions including a Privacy Officer who directly oversee data privacy compliance. More information can be found here:  
<https://www.financialforce.com/privacy/>
2. Where to find more information on data privacy compliance?
- a. <https://www.financialforce.com/privacy/>
3. Additional resources?
- a. Please see our Privacy FAQ for a primer on data privacy compliance at FinancialForce.  
<https://www.financialforce.com/privacy/financialforce-privacy-faq/>

For more information regarding the relevant attestation reports, assessments, certifications, and security frameworks applicable to FinancialForce, please refer to the section [Major Compliance Reports and Frameworks](#).