Critical Controls Implementation for Salesforce

Helping Organizations Securely Migrate to Salesforce Applications in the Cloud
The permanent and official location for the Enterprise Resource Planning Working Group is https://cloudsecurityalliance.org/working-groups/enterprise-resource-planning.
Acknowledgments

Lead Authors:
Frederik Weidemann
Sergio Abraham
Juan Perez-Etchegoyen

Reviewers:
Ivan Djordjevic

CSA Global Staff:
Shamun Mahmud

The Enterprise Resource Planning (ERP) WG seeks to develop best practices to enable organizations that run their business on large ERP implementations, such as SAP or Oracle applications, to securely migrate to and operate in cloud environments. Every ERP deployment is something that is unique to each organization. In most cases, organizations spend months, if not years, customizing their SAP or Oracle implementations and also spend a significant amount of money with third-party contractors to complete implementations. This makes standard security measures more difficult to implement due to the differences of each deployment. The complexity of these large implementations, combined with the criticality of data and processes housed in these applications, necessitates the establishment of industry best practices to provide security guidelines for companies migrating to the cloud, in order to protect the organizations’ critical infrastructure.
Table of Contents

Introduction .........................................................................................................................................5
How To Use This Document .................................................................................................................6
Controls Implementation .....................................................................................................................7
  USR01 - Secure Authentication ......................................................................................................7
  USR02 - User Accounts Management ............................................................................................9
  USR03 - Role-Based Access Control ............................................................................................10
  USR04 - Emergency Access .........................................................................................................12
  USR05 - Segregation of Duties .....................................................................................................14
  USR06 - Secure User Provisioning/Deprovisioning ....................................................................16
  USR07 - Accounts Security ..........................................................................................................18
  APP01 - Secure Landscape ...........................................................................................................20
  APP02 - Secure Baseline Configurations ......................................................................................21
  APP03 - Security Vulnerabilities ...................................................................................................23
  APP04 - Secure Communications ................................................................................................24
  APP05 - Change Management Controls .......................................................................................25
  APP06 - Secure Extensions ..........................................................................................................26
  INT01 - Secure Integrations and Application Programming Interface (API) .................................28
  DAT01 - Continuous Monitoring ...................................................................................................30
  DAT02 - Data Separation ..............................................................................................................32
  DAT03 - Data Encryption ..............................................................................................................34
  BUS01 - Inventory of Business Assets, Data, and Processes ........................................................35
  BUS02 - Business Process Controls .............................................................................................36
  BUS03 - Continuous Compliance ..................................................................................................37
Introduction

This paper will help an organization determine what security changes are needed when deploying Salesforce in the Cloud. For clarity, this paper will focus on the usage of the central Salesforce Platform. Salesforce itself can be heavily extended.

The target audience for this document is new adopters of Salesforce as well as existing Salesforce customers who want to achieve a baseline security.
How To Use This Document

This document is a reference to promote best practices for security operations in Salesforce. It does not replace Salesforce (the Vendor's) documentation and specific instructions, such as the Salesforce Security Guide.

Specifically, this document is to be used as part of the Cloud Security Alliance (CSA) Enterprise Resource Planning (ERP) Working Group's ongoing dialogue. Please refer to the ERP Working Group's site for additional resources.

Each of the twenty (20) controls presented in this document for the Salesforce Platform is directly mapped to CSA's overarching Top 20 Critical Controls for Cloud Enterprise Resource Planning Customers.

Two parts define each control:

- **Control Implementation**: The control implementation defines the rationale for the control. Information technology (IT) leaders and information security and compliance professionals will benefit from understanding and mapping each control into their overarching IT operational and security and compliance controls.

- **Checklist**: To implement each control, a checklist of specific requirements and/or steps are identified. Database administrators (DBAs) and system administrators can use this section to implement the control.

This document will use the words MUST, MUST NOT, SHOULD, SHOULD NOT, and MAY, as defined in RFC2119. MUST means that a checklist item is an absolute requirement. SHOULD means that the item is recommended to be implemented unless there are written reasons describing the full impact and context why the recommendation is not followed. MAY defines a truly optional item.

To make full use of this document, readers should be familiar with the CSA's Cloud Controls Matrix (CCM) and the Center for Internet Security's (CIS) Benchmarks for security hardening.
## Controls Implementation

<table>
<thead>
<tr>
<th>Domain</th>
<th>Salesforce</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control ID</td>
<td>USR01 - Secure Authentication</td>
</tr>
<tr>
<td>Technology Stack</td>
<td>Application</td>
</tr>
<tr>
<td>Versions</td>
<td>All</td>
</tr>
</tbody>
</table>

### Control Implementation

The authentication mechanism enabled for Salesforce must be configured securely so no one can impersonate application users. Best practices for this call for single sign-on, strong password policies, and using a strong second factor during the authentication process.

### Checklist/Steps in Order of Priority

The following attributes should be true for the authentication process:

1. **Multi-factor authentication with a strong second factor must be enforced.** Examples for weak factors are mails and SMS. Examples for strong factors are TOTP or the Salesforce Authenticator.
2. **Strong password policies should be enforced for all users, including end-users, technical users, and external users.** This should be achieved by enabling an organization-wide strong policy. Go to Setup and select ‘Password Policies’ in the Quickfind field. It’s possible to define a separate threshold for the password policy on profile level (e.g., for external users).
3. **If possible, single-sign should be enabled.**
4. **Improved security:**
   - For high-privilege generic users such as system administrators, passwords should be subject to significantly more stringent complexity requirements.
   - Login-IP restrictions and business hours should be set up for all profiles in use to reduce the attack surface.
References

- Salesforce Trailblazer Community | Salesforce Multi-Factor Authentication FAQ
- Salesforce Trailblazer Community | Set Password Policies
- Salesforce Trailhead | Secure Your Users' Identity
- Salesforce Trailblazer Community | View and Edit Password Policies in Profiles
- Salesforce Security Guide | Authenticate Users
<table>
<thead>
<tr>
<th>Domain</th>
<th>Salesforce</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control ID</td>
<td>USR02 - User Accounts Management</td>
</tr>
<tr>
<td>Technology Stack</td>
<td>Application</td>
</tr>
<tr>
<td>Versions</td>
<td>All</td>
</tr>
<tr>
<td>Control Implementation</td>
<td>Managing Salesforce user accounts is paramount for ensuring only the appropriate people have access. This control aims to assure that the user accounts that exist within the Salesforce organization are appropriately controlled and governed to avoid unauthorized access to business information.</td>
</tr>
</tbody>
</table>
| Checklist/Steps in Order of Priority | 1. Production user accounts must be changed and deactivated when creating a non-production sandbox for test and development purposes.  
2. User management should be centralized using a company-wide identity management system.  
3. Unused user accounts must be deactivated. User accounts may also be frozen, in which case record assignments will be untouched and the license won’t be freed.  
4. Because user accounts cannot be deleted, data should be anonymized if there are legal requirements. |
| References      | • Salesforce Trailblazer Community | Deactivate Users  
• Salesforce Trailblazer Community | Considerations for Deactivating Users  
• Salesforce Trailblazer Community | Data Protection and Privacy  
• Salesforce Trailblazer Community | Identity Connect  
• Salesforce Trailblazer Community | Manage Salesforce User Identities with SCIM  
• Salesforce Trailblazer Community | Let Users Scramble Their User Data  
• Salesforce Apex Reference Guide | UserManagement Class |
Role-based access control (RBAC) should be used to manage Salesforce permissions. Salesforce can support RBAC functionality that allows users in the same functional or technical area to have the same authorizations bundled together in a profile assigned to users. Further assignments can be done using permission sets.

Access to Salesforce objects can be generally defined using object permissions. Further restrictions can be made at the field level. Finally, access to individual records can be defined using sharing rules. In addition, access to records can be controlled using hierarchies based on roles. Roles act as an inheritance level for granting access to records for certain Salesforce objects. Therefore, roles behave differently than in other systems and, in general, profile and permission sets are comparable to what in other IT systems is named a role.

The Salesforce suite needs to be continuously monitored to ensure that users have only the minimal number of appropriate permissions they need for their day-to-day business – this is the principle of least privilege.

The most important topic for implementation of this control is to screen the change management process of user, permissions, roles, and responsibilities (e.g., when an employee changes position and the employee's authorization needs to be changed). A process should be established for when an HR change to a position happens. A new hire, as well as a termination, should be monitored to take appropriate action. As in other applications, if these types of changes are not properly controlled it can lead to users with powerful privileges due to cumulative permissions from different permission sets and profiles.
Checklist/Steps in Order of Priority

1. Permission assignments must follow the “least privilege principle.” Therefore, only the permissions that are required for the target user must be assigned.

2. A control for the “administrators can login as any user” feature must be defined. This feature allows administrators to login as any user and impersonate them without a requirement to get the user’s consent.

3. Usage of the “login as any user” feature should be automatically monitored by analyzing the Setup and Audit Trail.

4. Set up a control for permission assignments that validates the least privilege principle assignment and that ensures that segregation of duty conflicts do not happen.

References

- Salesforce Security Guide | Give Users Access to Data
- Salesforce Trailblazer Community | Controlling Access Using Hierarchies
<table>
<thead>
<tr>
<th>Domain</th>
<th>Salesforce</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control ID</td>
<td>USR04 - Emergency Access</td>
</tr>
<tr>
<td>Technology Stack</td>
<td>Application</td>
</tr>
<tr>
<td>Versions</td>
<td>All</td>
</tr>
</tbody>
</table>

**Control Implementation**

Emergency access is granted to staff upon system failures or errors or in the ordinary course of business as a consequence of staff unavailability, such as for sick leave, vacation, termination, etc. Granting emergency access often results in privileges normally prohibited, exposing the entity to additional risk which must be appropriately managed.

1. Define an emergency access policy that describes who can do what along with when, where, and how. Address responsibilities for emergency access administration, access granting, monitoring, termination, reporting, and auditing. Granting of emergency access must be risk-based and consider segregation of duties and least privilege.

2. A policy should be defined that consists of the following areas:
   - Administration: Who manages the emergency access process?
   - Grant access: Who can approve and for what activities?
   - Monitor access: What gets reported, when, to whom, and how?
   - Terminate access: Who can approve?
   - Report and audit access: What, when, to whom, and how?

**Checklist/Steps in Order of Priority**

1. **Overall**
   - Determine access requirements for the emergency access requested.
   - Require a service request (ticket) for all emergency access activities. Utilize approval workflows and audit for effectiveness.
   - Identify accounts within the application and supporting technologies that are in scope for emergency access.
• For accounts identified for emergency use, ensure that long, complex passwords are in use, to force the use of a password safe. Confirm the use of both complex passwords and an enterprise password safe.
• Stream audit logs (Setup Audit Trail and Login History) to a SIEM for correlation to identify emergency use of identified accounts without service requests and/or a password safe activity. Access to the transactional logs requires an additional commercial license from Salesforce. Access to the emergency user should be login-restricted towards the outgoing IP of the terminal server.
• Implement a regular reporting and audit procedure for all emergency access activities.

2. Improved Security
• For pulling an emergency user password safely, a service request (ticket) should be referenced. Ensure that the service request is assigned to the same person pulling the password.

References
• Salesforce Trailblazer Community | Monitor Login History
• Salesforce Trailblazer Community | Enable Event Monitoring
• Salesforce Trailblazer Community | Require Users to Log In with SSO
<table>
<thead>
<tr>
<th>Domain</th>
<th>Salesforce</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control ID</td>
<td>USR05 - Segregation of Duties</td>
</tr>
<tr>
<td>Technology Stack</td>
<td>Application</td>
</tr>
<tr>
<td>Versions</td>
<td>All</td>
</tr>
<tr>
<td>Control Implementation</td>
<td></td>
</tr>
</tbody>
</table>

Segregation of duties (SOD) is a control principle that supports the idea that no one should control a process from beginning to end. This control intends to prevent conflict of interest, fraud, error, and malicious acts. Within any process, no one should have the ability to perform more than one incompatible task, such as creating and approving an action. For example, someone should not be allowed to create a fictitious order to cover up a fraudulent delivery or shipment. SOD entails walking a line between task and employee flexibility and security.

An SOD matrix can implement segregation of duties in the ERP. The matrix should be reviewed and approved – internally and externally – by auditors. Additionally, access should be requested electronically with SOD verification by the system. Failed verifications should be flagged, reported, and returned for resolution, while SOD-verified requests are forwarded to appropriate personnel for review, approval, and activation. The system should continually monitor transaction usage and automatically generate a report each time a person performs an incompatible transaction.

Regardless of the service model, ensuring the adequate segregation of duties is always the responsibility of the customer.

<table>
<thead>
<tr>
<th>Checklist/Steps in Order of Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. SOD conflicts must be documented using an SOD matrix.</td>
</tr>
<tr>
<td>2. Preventive SOD checks should be in place when permissions are being assigned.</td>
</tr>
<tr>
<td>3. All users with their assigned permissions should be continuously monitored for SOD defects.</td>
</tr>
<tr>
<td>4. Monitor sensitive transaction usage, including alerting and reporting.</td>
</tr>
<tr>
<td>References</td>
</tr>
<tr>
<td>------------</td>
</tr>
<tr>
<td>• Salesforce Trailblazer Community - Administrators and Separation of Duties</td>
</tr>
<tr>
<td>Domain</td>
</tr>
<tr>
<td>-----------------</td>
</tr>
<tr>
<td>Control ID</td>
</tr>
<tr>
<td>Technology Stack</td>
</tr>
<tr>
<td>Versions</td>
</tr>
</tbody>
</table>
| Control Implementation | Provisioning technical and functional users within a Salesforce organization is a crucial security control from an operational perspective. The provisioning process needs to ensure:  
1. There is a valid business reason and requirement behind the creation of the user.  
2. The user is created in the appropriate organization.  
3. There is a responsible person associated with this account.  
4. User permissions (authorizations) are assigned according to the least privilege approach.  
5. There is a validity period defined whenever applicable to the account.  

Unmanaged and dormant accounts could be misused to access the system in an unauthorized way. Therefore, user accounts’ deprovisioning must be managed appropriately. |
| Checklist/Steps in Order of Priority | 1. The provisioning and deprovisioning of users must be appropriately managed and documented in company policy. Relevant compliance requirements must be met; examples are ISO/IEC 27001, NIST Cybersecurity Framework, or the PCI DSS (Payment Card Industry Data Security Standard).  
2. The least privilege principle must be enforced when permissions are assigned. Each user should have only those permissions assigned that are required for their business activities.  
3. Monitor the organization for inactive accounts. |
References

• Salesforce Trailblazer Community | Security Center Metrics, User and Profile Metrics
• Salesforce Trailblazer Community | Identity Connect
• Salesforce Trailblazer Community | Manage Salesforce User Identities with SCIM
The security of Salesforce user accounts is paramount, especially if an on-premise application is migrated to the Salesforce cloud. Login processes should be developed to successfully make it more difficult for adversaries to enter the Salesforce organization using valid but compromised credentials.

Additionally, the Salesforce organization should implement session management mechanisms according to the applicable standards.

Organizations using Salesforce should make sure to:

1. Enable multi-factor authentication.
2. Enable the passwords to rule, prioritizing password length rather than complexity.
3. Analyze user login behavior to detect unfamiliar login location, time, etc. Also, link to other user activities (e.g., data provided through cloud access and security broker providers, as well as conditional access).
4. Implement single sign-on property.
5. Limit access to the ERP system from specific networks.
6. Ensure session tokens are dynamic, sufficiently random, encrypted, and expire on time.
7. Enable audit logging of user activities and transactions (read-only to all, including administrators).

1. Enable encryption between client and server to protect user credentials.
2. Multi-factor authentication must be enforced for all users.
3. Where multi-factor authentication is not supported, compensating controls must be in place (e.g., IP login limitations).
4. Send login logs to a centralized log server.
5. Monitor the centralized log server using an SIEM product.

References

- Center for Internet Security | CIS Controls
- NCSC | Cloud Security Guidance
- Salesforce Security Guide
- NIST | Special Publication 800-63B Digital Identity Guidelines
Due to the criticality of Salesforce, applications are typically deployed in a multi-tiered environment where development and testing are performed in dedicated systems. Risks affecting the entire landscape – in terms of secure settings, isolation, interfaces, and access – could potentially alter the integrity and security of the production environment.

Processes must be implemented across the landscape to ensure no unauthorized access to the production environment is allowed. These may include:

- Prevent access and authorization risks in cross-enterprise systems/platforms.
- Ensure roles and responsibilities are well defined.
- Ensure the same level of security is implemented across all environments to avoid escalation of privileges across the landscape.

Regardless of the service model, this control is always the responsibility of the customer.

<table>
<thead>
<tr>
<th>Checklist/Steps in Order of Priority</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Inventory all in-scope governance policies and controls for Salesforce.</td>
<td></td>
</tr>
<tr>
<td>2. Determine ownership (team) of the policies and related controls.</td>
<td></td>
</tr>
<tr>
<td>3. Assess the effectiveness of current policies.</td>
<td></td>
</tr>
<tr>
<td>4. Set up a regular review and update process to be able to adapt to new compliance requirements.</td>
<td></td>
</tr>
<tr>
<td>5. Automated controls should be implemented where applicable.</td>
<td></td>
</tr>
</tbody>
</table>

References

Not applicable
### Domain
Salesforce

### Control ID
APP02 - Secure Baseline Configurations

### Technology Stack
Application

### Versions
All

### Control Implementation
Salesforce environments can be complex and consist of several different solutions. Those components can closely interact with each other and can be extensively customizable and configurable. While the extensibility of the Salesforce platform is a compelling advantage, a significant percentage of the possible number of configuration options have a material security impact. Therefore, a best practice security process should consist of:

1. Defining baselines for all components and technologies.
2. Enforcing the baselines.
3. Automating baseline enforcement and monitoring where applicable.
4. Setting up review and update procedures

### Checklist/Steps in Order of Priority

1. A secure baseline policy must be defined.
2. The baseline policy should consist of the following areas:
   - Security configuration
   - Authentication
   - Authorizations & critical permissions
   - Interfaces (data in transit)
   - Asset protection (data in rest)
   - Network requirements
   - Logging
   - Monitoring
   - Custom development (e.g. APEX)
   - Security patch policy
   - Change management
   - Applicable regulatory compliance requirements
   - Audit and fraud protection procedures
   - Security governance framework
- Risk management procedures
- Operational security procedures
- Data classification/categorization

References

- NIST Computer Security Resource Center | NIST Risk Management Framework SP 800-53 Revision 5.1: CM-6(1)
- Salesforce Trailhead | Use Health Check to Scan Your Security Configurations
<table>
<thead>
<tr>
<th>Domain</th>
<th>Salesforce</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control ID</td>
<td>APP03 - Security Vulnerabilities</td>
</tr>
<tr>
<td>Technology Stack</td>
<td>Application</td>
</tr>
<tr>
<td>Versions</td>
<td>All</td>
</tr>
<tr>
<td>Control Implementation</td>
<td>Salesforce periodically provides patches to fix security vulnerabilities in its code through release versions (formerly named “critical updates”). While the infrastructure is maintained by Salesforce for the customer, the application level may require the customer to perform tasks prior to the activation of a security enhancement. Salesforce will inform the customer what is changing, the corresponding impact to the organization, and until when the preparation steps need to be done. It's not possible to opt out of a security enhancement, but missing required preparation steps may impact your organization and can result in activating a new version.</td>
</tr>
</tbody>
</table>
| Checklist/Steps in Order of Priority | 1. A continuous vulnerability management process must be set up for security alerts and release updates.  
2. Each change should be tested in a sandbox organization.  
3. It’s recommended to activate security enhancements in production during off-peak hours. |
| References   | • Salesforce Trailblazer Community | Release Updates  
• Salesforce Trailblazer Community | Keep Up with Security Alerts  
• Salesforce Trailblazer Community | Manage Security Contacts for Your Organization  
• Salesforce Trailblazer Community | Manage Your Notification Preferences in the Salesforce Help Portal |
<table>
<thead>
<tr>
<th>Domain</th>
<th>Salesforce</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control ID</td>
<td>APP04 - Secure Communications</td>
</tr>
<tr>
<td>Technology Stack</td>
<td>Application, Network</td>
</tr>
<tr>
<td>Versions</td>
<td>All</td>
</tr>
<tr>
<td>Control Implementation</td>
<td>In a Salesforce environment, there are multiple ways to communicate with the application, including internet browsers (HTTP), mobile applications, and API access. All data in transit must be protected using encryption.</td>
</tr>
<tr>
<td>Checklist/Steps in Order of Priority</td>
<td><strong>Application</strong>&lt;br&gt;1. All data in transit must be protected using encryption. This includes both internal and external communications.&lt;br&gt;2. Outgoing APEX callouts should use https.&lt;br&gt;3. Data flowing towards external connected applications (e.g., via AppExchange or interfaces) must be equally protected. Example: Salesforce doesn't allow access via unencrypted FTP.&lt;br&gt;4. For improved security, login IP restrictions may be used to limit the surface for the attacker.&lt;br&gt;Remarks:&lt;br&gt;5. Ciphersuites and encryption settings are handled by Salesforce.</td>
</tr>
<tr>
<td>References</td>
<td>• NIST Computer Security Resource Center</td>
</tr>
<tr>
<td>Domain</td>
<td>Salesforce</td>
</tr>
<tr>
<td>--------------</td>
<td>------------</td>
</tr>
<tr>
<td>Control ID</td>
<td>APP05 - Change Management Controls</td>
</tr>
<tr>
<td>Technology Stack</td>
<td>Application</td>
</tr>
<tr>
<td>Versions</td>
<td>All</td>
</tr>
<tr>
<td>Control Implementation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Appropriate change management controls should be implemented across all components of the Salesforce organization so that no unmanaged changes can be implemented in the production system through unauthorized access. Any planned changes should have a defined scope and their impact should be evaluated. Prior to go live, any metadata and custom coding changes should be tested.</td>
</tr>
<tr>
<td>Checklist/Steps in Order of Priority</td>
<td></td>
</tr>
<tr>
<td>1.</td>
<td>Any change must be tested in a sandbox.</td>
</tr>
<tr>
<td>2.</td>
<td>Any change must be subject to a security review.</td>
</tr>
<tr>
<td>3.</td>
<td>Changes should be tracked using a version control system (e.g., GIT).</td>
</tr>
<tr>
<td>4.</td>
<td>Any change should be subject to a UAT prior to deployment.</td>
</tr>
<tr>
<td>5.</td>
<td>Deployment to production should be done based on the approved artifacts in the version control system.</td>
</tr>
<tr>
<td>6.</td>
<td>Any change should be communicated in the organization.</td>
</tr>
<tr>
<td>7.</td>
<td>Permissions should be restricted in production so that only the technical deployment users are able to perform changes.</td>
</tr>
<tr>
<td>8.</td>
<td>A regularly performed cloning process should be used to create a pre-production staging sandbox for testing.</td>
</tr>
<tr>
<td>9.</td>
<td>For improved security, any manual changes in production should be automatically reverted to the latest setting persisted in the version control system.</td>
</tr>
<tr>
<td>References</td>
<td></td>
</tr>
<tr>
<td>- Salesforce</td>
<td>Best Practices for Salesforce Change Management</td>
</tr>
<tr>
<td>- Salesforce Trailhead</td>
<td>Architect Journey: Development Lifecycle and Deployment</td>
</tr>
<tr>
<td>- Salesforce Trailhead</td>
<td>Determine Which Application Lifecycle Management Model Is Right for You</td>
</tr>
<tr>
<td>- Salesforce Dreamforce To You 2020</td>
<td>Sandbox Best Practices for Developers</td>
</tr>
</tbody>
</table>
Salesforce can be heavily extended with applications available in the AppExchange marketplace and through custom development using APEX.

Applications offered in the AppExchange marketplace must pass a security review. This review is automated and Salesforce suggests that partners perform manual testing too. Therefore, it's not implicit that an application hosted in AppExchange meets the same security standards as the Salesforce platform itself. Security checks that are best performed manually rather than automated may not have been done. Examples include: design failures, logical errors, and not meeting legal requirements.

Similarly, Salesforce customers must ensure that secure development best practices are met when using custom APEX coding.

1. Create and enforce a secure development and coding guidelines document.
2. Setup a secure software development lifecycle, including a mandatory review process for all developed artifacts.
3. All software developments must use a version control system.
4. For external application, a risk assessment should be conducted to ensure that security and compliance requirements are met.
5. External applications must always be installed only for administrators. Permissions must set afterwards according to the least privilege principle.
References

- Salesforce Apex Developer Guide | Apex Security and Sharing
- Salesforce Apex Developer Guide | Security Tips for Apex and Visualforce Development
- Salesforce Trailblazer Community | Monitor Setup Changes with Setup Audit Trail
<table>
<thead>
<tr>
<th>Domain</th>
<th>Salesforce</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control ID</td>
<td>INT01 - Secure Integrations and Application Programming Interface (API)</td>
</tr>
<tr>
<td>Technology Stack</td>
<td>Application</td>
</tr>
<tr>
<td>Versions</td>
<td>All</td>
</tr>
<tr>
<td>Control Implementation</td>
<td>The extensive integration of Salesforce with external applications and data sources is common practice because of the nature of processes supported by these systems. In a typical Salesforce environment, there are interfaces and connections between different solutions and different environments. If improperly secured, these integrations are ripe for abuse and production information and data risks may be easily compromised. The management of Salesforce interfaces should address the following considerations: 1. Asset management 2. Continuous security monitoring of all interfaces</td>
</tr>
<tr>
<td>Checklist/Steps in Order of Priority</td>
<td>1. Maintain an inventory of all interfaces, including the type of exchanged data and the technical details of the connections, such as protocol, user, business owner, authorizations, and encryption details. 2. Set up a continuous process for security monitoring of the interfaces. • Avoid using insecurely provisioned interfaces, such as broad trust relationships or the utilization of usernames and passwords that others can leverage. Best practice is to dedicate one technical user account (service account) to each interface.</td>
</tr>
</tbody>
</table>
• Always apply the “least privilege” principle to define the privileges that technical users will be granted for various interfaces.
• Encrypt all communication flowing through interfaces.
• Interfaces should not be established from lower security systems (such as development) to systems with higher security (such as production) if there are persisted credentials or access tokens in the development system.
• If secrets are used to set up the interfaces (i.e., API keys, passwords, certificates), establish the proper management process to govern those secrets (maintain/change/rotate if needed).
• Detect and remove obsolete interfaces and integrations.

References

• Center for Internet Security | The 18 CIS Controls
• Salesforce Integration Patterns and Practices | Integration Patterns Overview
A complex bundle of multiple applications and services is offered by Salesforce. To understand what is happening within Salesforce, different log providers must be analyzed and licensed. To be effective, these sources need to be fed to a security information and event management (SIEM) system. Alerts should be set up and handled by an incident response process.

In addition, transactional security policies can be utilized to perform alerts when certain conditions are met, such as when an emergency user logs on. If possible, configure policies to intercept real-time events and apply appropriate actions (see Enhanced Transaction Security reference, below).

1. Enable application logging and auditing. The following events must be covered:
   - Access and unsuccessful logins are tracked in the “Login History” for up to six months. Enable additional login forensics by enabling storing in the Event Manager. Furthermore, Log Out events can be tracked using the Event Manager (see Real-Time Event Monitoring and Enable Event Monitoring references, below).
   - Metadata configuration changes are tracked in the “Setup Audit Trail” – ensure that Sign-On-Audit is set to “Forms level” to track and log which professional forms users visit. Also ensure this log is forwarded to the centralized log solution.
2. Enable application logging and auditing. The following events should be covered:

   - Additional transactional logs are available if they’re licensed separately – these provide the following event types (see Real-Time Event Monitoring Data Streaming and Storage references below for additional details):
     - API Anomaly Event
     - API Event
     - Bulk API Result Event
     - Concurrent Long Running Apex Error Event
     - Credential Stuffing Event
     - Identity Provider Event
     - Identity Verification Event
     - Lightning URI Event
     - List View Event
     - Login Event
     - LoginAs Event
     - Logout Event
     - Report Anomaly Event
     - Report Event
     - Session Hijacking Event
     - URI Event

3. For individual business logging requirements, Field History Tracking should be evaluated, which will track modifications to a defined list of Salesforce and custom objects.

4. A centralized logging solution must be used, to which all logs are forwarded.

5. Implement a process to review the logs automatically, preferably using a SIEM tool, so a timely response is possible.

6. Implement an incident response process so whenever an incident is identified the good teams are involved in containing the incident.

References

- Salesforce Trailblazer Community | Enable Login Forensics
- Salesforce Trailblazer Community | Monitor Setup Changes with Setup Audit Trail
- Salesforce Trailblazer Community | Field History Tracking
- Salesforce Trailblazer Community | Enhanced Transaction Security
- Salesforce Trailblazer Community | Real-Time Event Monitoring
- Salesforce Trailblazer Community | Enable Event Monitoring
- Salesforce Trailblazer Community | Real-Time Event Monitoring Data Streaming
- Salesforce Trailblazer Community | Real-Time Event Monitoring Data Storage
### Domain
Salesforce

### Control ID
DAT02 - Data Separation

### Technology Stack
Database

### Versions
All

### Control Implementation
Salesforce implementations are usually composed of multiple environments that have diverse roles, such as sandbox, development, quality assurance, or production – to name a few. The security of the overall environment is paramount to the security of the data that is hosted in the production system. Likewise, organizations have fiduciary responsibilities to protect data wherever it exists.

In general terms, access to lower-risk environments such as development should not place sensitive data at risk. This means that, as much as possible, production and non-production environments should be separated (with different access controls) and that, unless sensitive information in non-production environments is appropriately secured (e.g., masked, scrambled, and/or redacted), these environments be secured with the same level and standards of protection.

1. Production data must be legally protected wherever it exists. When production data is being copied to a non-production system the data must be treated and protected as it is in the production system. Custom solutions can also be used to mask, scramble, or redact PII data. Example: all personal data is copied to a test system, then this test system is treated similarly to a production system.

Data classification can be used to assign sensitivity levels to fields in Salesforce, which can help guide some decisions around the level of users’ access to data as well as masking strategies before moving data off production and onto sandbox environments (see references below).
2. All user accounts should be either changed or deactivated when creating copies of production for test, development, and support databases.

3. Responsibilities (roles) used only in test and development must be disabled in production. Support and development roles are commonly created with elevated authorizations not allowed in production.

4. Interfaces between non-production environments and production systems should not exist. Interfaces may be used on a case-by-case evaluation and must meet all compliance requirements (e.g., encryption and least privilege principle). Interfaces should be pointed from production to non-production (push data) rather than from non-production to production (pull data).

References

- Salesforce Trailblazer Community | Classify Sensitive Data to Support Data Management Policies
- Salesforce Security Guide | Give Users Access to Data
- Salesforce Trailblazer Community | Secure Your Sandbox Data with Salesforce Data Mask
<table>
<thead>
<tr>
<th>Domain</th>
<th>Salesforce</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control ID</td>
<td>DAT03 - Data Encryption</td>
</tr>
<tr>
<td>Technology Stack</td>
<td>Application</td>
</tr>
<tr>
<td>Versions</td>
<td>All</td>
</tr>
<tr>
<td>Control Implementation</td>
<td>Business data stored and processed by Salesforce is its most crucial component. According to predefined rules and policies, sensitive data at rest should be encrypted and must be classified to avoid unauthorized access. Salesforce Shield offers additional layers of data protection including platform encryption, full event monitoring, and field audit trail to track changes of the data. For companies handling sensitive data, such as financial service companies or healthcare companies, it should be evaluated if Shield is necessary to fulfill compliance requirements. Concerning business data, data should be encrypted depending on the classification while at rest and when stored in any other location.</td>
</tr>
<tr>
<td>Checklist/Steps in Order of Priority</td>
<td>1. All business data must be classified (see Classify Sensitive Data reference below) and an owner should be assigned. 2. Data should be encrypted at rest according to the company's applicable compliance requirements.</td>
</tr>
<tr>
<td>References</td>
<td></td>
</tr>
</tbody>
</table>
  - Salesforce | Salesforce Shield  
  - Salesforce Trailblazer Community | Classify Sensitive Data to Support Data Management Policies  
  - Salesforce Trailhead | Secure Your Apps with Salesforce Shield  
  - Salesforce Trailblazer Community | Strengthen Your Data's Security with Shield Platform Encryption |
<table>
<thead>
<tr>
<th>Domain</th>
<th>Salesforce Business Processes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control ID</td>
<td>BUS01 - Inventory of Business Assets, Data, and Processes</td>
</tr>
<tr>
<td>Technology Stack</td>
<td>Application</td>
</tr>
<tr>
<td>Versions</td>
<td>All</td>
</tr>
<tr>
<td>Control Implementation</td>
<td>Protecting business data stored and processed by the Salesforce application is one of the most challenging parts of operating business applications at scale. It is important to have the right level of visibility around the data and the processes that each application is supporting. Having a clear inventory of these components is the starting point to understanding where the crown jewels are in an organization and to providing the right governance and controls around those components. An inventory of applications, data, and processes should be implemented to serve as a single source of truth regarding business processes.</td>
</tr>
<tr>
<td>Checklist/Steps in Order of Priority</td>
<td>1. Ensure a single source of truth exists (inventory/repository), such as an ITIL Configuration Management Database (CMDB). 2. Identify and thoroughly document all the supporting technologies and components that build up both the production and non-production Salesforce environments. Incorporate critical relationships with other applications such as Service Cloud, Marketing, or others. 3. Ensure that service level agreements are defined for all Salesforce applications and supporting technologies. 4. Ensure that for each Salesforce environment there is a risk management scorecard available, inclusive of sensitive data protection requirements (See Classify Sensitive Data reference below).</td>
</tr>
</tbody>
</table>
| References          | • ISO 27001:2013 | A.8.1 - Asset Management  
• Salesforce Trailblazer Community | Classify Sensitive Data to Support Data Management Policies |
<table>
<thead>
<tr>
<th>Domain</th>
<th>Salesforce Business Processes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control ID</td>
<td>BUS02 - Business Process Controls</td>
</tr>
<tr>
<td>Technology Stack</td>
<td>Application</td>
</tr>
<tr>
<td>Versions</td>
<td>All</td>
</tr>
<tr>
<td>Control Implementation</td>
<td>Salesforce supports critical business processes. Controls must be put in place to ensure that no fraudulent activities can be executed by abusing existing or elevated privileges.</td>
</tr>
</tbody>
</table>
| Checklist/Steps in Order of Priority | 1. Together with the business process owners, critical steps in each critical business process within Salesforce must be identified.  
2. For each process, all requirements for the organization’s fraud protection program should be met. |
<p>| References    | Not applicable               |</p>
<table>
<thead>
<tr>
<th>Domain</th>
<th>Salesforce Business Processes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control ID</td>
<td>BUS03 - Continuous Compliance</td>
</tr>
<tr>
<td>Technology Stack</td>
<td>Application</td>
</tr>
<tr>
<td>Versions</td>
<td>All</td>
</tr>
<tr>
<td>Control Implementation</td>
<td>Due to the nature of data and processes supported by Salesforce, it is critical to maintain certain compliance levels with the regulations that apply to the data, processes, and industry that the organization operates. Implement a process that ensures continuous compliance and can work as a centralized view to monitor control effectiveness in real time. Additionally, official Salesforce documentation for security and compliance of Salesforce services should be reviewed and incorporated as part of the compliance controls framework (see Certifications, Standards, and Regulations and Trust and Compliance Documentation references, below).</td>
</tr>
<tr>
<td>Checklist/Steps in Order of Priority</td>
<td>1. All compliance, regulatory standards as well as contractual agreements that are affecting the Salesforce Applications must be identified. 2. Mandatory critical controls must be identified. 3. A governance framework that includes auditing must be established. 4. Automated testing procedures that can validate control effectiveness 24x7 should be established. 5. An alerting mechanism should be implemented to address findings as soon as they happen.</td>
</tr>
</tbody>
</table>
| References | • Salesforce | Certifications, Standards and Regulations  
• Salesforce | Trust and Compliance Documentation  
• Wikipedia | Continuous Monitoring  
• Wikipedia | Continuous Auditing  
• Wikipedia | Regulatory Compliance |