CIS Controls Gap Assessment Report

CloudStrategik Consulting

Effective Date: August 7, 2024
Version: 1.1

Prepared by: CloudStrategik Consulting
Anderson@cloudstrategik.com

Confidentiality Statement

This document contains proprietary and confidential information of CloudStrategik Consulting. The information contained herein is disclosed to the recipient in confidence for the sole purpose of internal use. No part of this document may be disclosed, reproduced, or distributed without the prior written consent of CloudStrategik Consulting.

Policy Title:	CIS Controls Gap Assessment Report
Policy Owner:	Anderson Anthony, Chief Compliance Officer
Effective Date:	August 7, 2024
Revised Date:	August 7, 2024

Contents

1 Executive Summary

This report provides a comprehensive assessment of the current security controls in place within our Salesforce org against the CIS Controls framework. Key findings include:

- 70% of CIS Controls are fully or partially implemented.
- Critical gaps exist in administrative privilege management and application software security.
- Salesforce-specific security features like Field-Level Security and Sharing Rules are well-implemented.
- Multi-Factor Authentication (MFA) adoption is at 60%, below the recommended 100%.

Priority areas for improvement include enhancing account monitoring, implementing stricter password policies, and conducting more frequent security awareness training.

2 Introduction

This report provides a comprehensive assessment of the current security controls in place within the Salesforce org against the CIS Controls framework. The objective is to identify areas of improvement and ensure alignment with best practices.

3 Purpose

The purpose of this assessment is to provide a framework for evaluating the security posture of the Salesforce org. It outlines the existing controls, identifies gaps, and provides recommendations to enhance compliance with the CIS Controls.

4 Scope

This assessment applies to all components within the Salesforce org, including users, profiles, permission sets, roles, and configurations. It encompasses all activities related to the management and security of these components.

5 Definitions

- **CIS Controls**: A set of best practices for securing IT systems and data, developed by the Center for Internet Security.
- **Gap Analysis**: The process of comparing current controls with required controls to identify areas that need improvement.

- **Salesforce Org**: The Salesforce organization, including all its users, roles, profiles, and configurations.
- **MFA**: Multi-Factor Authentication, an additional layer of security beyond username and password.
- **Field-Level Security**: Salesforce feature that restricts users' access to view and edit specific fields.
- **Sharing Rules**: Salesforce feature that allows record access to users who would not typically have access through the organization's sharing model.

6 Methodology

The assessment involved collecting data on existing controls within the Salesforce org, mapping these controls to the CIS Controls framework, and identifying gaps where controls are either missing or inadequate. The following data sources were used:

- User data
- Profile data
- Permission sets data
- Roles data
- Permission set assignments data
- Salesforce security settings
- Salesforce Shield Event Monitoring logs

7 Salesforce Org Overview

The Salesforce org assessed in this report includes the following components:

- **Users**: A total of 500 active users with various roles and profiles.
- **Profiles**: 20 distinct profiles that define permissions and access levels.
- **Permission Sets**: 15 permission sets that provide additional privileges to specific users.
- **Roles**: A hierarchical structure of 10 roles that define reporting and data access levels.
- **Permission Set Assignments**: Assignments of permission sets to users for enhanced access control.
- **Custom Objects**: 25 custom objects, some containing sensitive data.
- **AppExchange Apps**: 5 third-party applications installed from the AppExchange.

8 Gap Analysis Results

The following table summarizes the gap analysis results, mapping the current controls to the CIS Controls and identifying any gaps.

CIS Control	Description	Status	Risk
1	Inventory of Hardware Assets	N/A	Low
2	Inventory of Software Assets	Partial	Medium
3	Continuous Vulnerability Management	Full	Low
4	Controlled Admin Privileges	Partial	High
5	Secure Config for Hardware/Software	Partial	Medium
6	Maintenance and Monitoring of Logs	Full	Low
7	Email and Web Browser Protections	N/A	Low
8	Malware Defenses	Full	Low
9	Limitation of Network Ports	Partial	Medium
10	Data Recovery Capabilities	Full	Low
11	Secure Config for Network Devices	Partial	Medium
12	Boundary Defense	Partial	High
13	Data Protection	Full	Low
14	Controlled Access Based on Need	Full	Low
15	Wireless Access Control	N/A	Low
16	Account Monitoring and Control	Partial	High
17	Security Awareness Training	Partial	Medium
18	Application Software Security	Partial	High
19	Incident Response and Management	Full	Low
20	Penetration Tests and Red Team	Partial	Medium

9 Detailed Findings

Inventory and Control of Hardware Assets

Description: Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access.
Status: Not Applicable
Risk Rating: Low
Details: This control is not applicable as it pertains to physical hardware assets, which are not managed within the Salesforce org.

Inventory and Control of Software Assets

Description: Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute.
Status: Partially Implemented
Risk Rating: Medium
Details: Software inventory is maintained for applications installed on user devices, but not all software is tracked at the granular level required. Steps need to be taken to ensure comprehensive software inventory management.
Salesforce-Specific Findings:

- 5 third-party AppExchange applications are installed.
- No formal process exists for vetting and approving new AppExchange installations.

Recommendations:

- Implement a system to track all installed software versions and patches.
- Establish a formal process for vetting and approving AppExchange applications.
- Conduct regular security reviews of all installed applications.
- Utilize Salesforce's Package Manager to monitor and control package versions.

Continuous Vulnerability Management

Description: Continuously acquire, assess, and take action on information regarding new software vulnerabilities and threats.
Status: Fully Implemented
Risk Rating: Low
Details: Continuous vulnerability management is in place, with regular scanning and patching of software vulnerabilities. Automated tools are used to identify and remediate vulnerabilities promptly.
Salesforce-Specific Findings:

- Salesforce Security Health Check is run monthly with a current score of 85%.
- All critical security updates are applied within 30 days of release.

Recommendations:

- Continue current practices.
- Consider increasing the frequency of Security Health Check runs to weekly.
- Implement automated alerts for new Salesforce security patches and updates.

Controlled Use of Administrative Privileges

Description: Use processes and tools to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.
Status: Partially Implemented
Risk Rating: High
Details: Administrative privileges are tracked and controlled for most systems, but some gaps exist in monitoring and auditing the use of these privileges. Additional controls and regular reviews are needed to ensure complete adherence to this control.
Salesforce-Specific Findings:

- 15% of users (75 users) have administrative privileges, which is higher than recommended.
- No formal process exists for regularly reviewing and adjusting administrative access.

Recommendations:

- Implement least privilege principles for administrative accounts.
- Reduce the number of users with administrative privileges to less than 5% of total users.
- Conduct quarterly audits to review and adjust administrative privileges.
- Implement Salesforce Shield for enhanced monitoring of administrative actions.
- Utilize Salesforce's Delegated Administration feature to assign limited administrative privileges.

Secure Configuration for Hardware and Software

Description: Establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process.
Status: Partially Implemented
Risk Rating: Medium
Details: While secure configurations are enforced for many systems, not all configurations are consistently managed. A more rigorous configuration management process is required to ensure that all systems adhere to security standards.
Salesforce-Specific Findings:

- Salesforce security settings are generally well-configured, but some improvements are needed.
- Session security settings are not optimized (2-hour timeout instead of recommended 1 hour).

Recommendations:

- Implement stricter session security settings (reduce timeout to 1 hour).

- Enable Salesforce's TLS 1.2 encryption for all connections.
- Regularly review and update Salesforce security settings using the Security Health Check feature.
- Implement change management processes for Salesforce configuration changes.

Maintenance, Monitoring, and Analysis of Audit Logs

Description: Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.
Status: Fully Implemented
Risk Rating: Low
Details: Audit logs are collected and monitored continuously. The organization employs tools to analyze logs for suspicious activities and potential security incidents.
Salesforce-Specific Findings:

- Salesforce Event Monitoring is implemented and actively used.
- Automated alerts are set up for critical events like multiple failed login attempts.

Recommendations:

- Continue current practices.
- Consider implementing Salesforce Shield for enhanced event monitoring and auditing capabilities.
- Regularly review and refine event monitoring rules and alerts.

Email and Web Browser Protections

Description: Improve protections for the use of web browsers and email clients.
Status: Not Applicable
Risk Rating: Low
Details: This control is not applicable as email and web browser protections are managed outside of the Salesforce org.

Malware Defenses

Description: Control the installation, spread, and execution of malicious code at multiple points in the enterprise.
Status: Fully Implemented
Risk Rating: Low
Details: Robust malware defenses are in place, including antivirus software, endpoint protection, and regular updates. These defenses are regularly tested and updated to counter new threats.
Salesforce-Specific Findings:

- Salesforce's built-in malware protection is active for all file uploads.

- Custom validation rules are in place to prevent malicious code injection in text fields.

Recommendations:

- Continue regular updates and testing of malware defenses.
- Conduct periodic reviews to ensure the effectiveness of Salesforce's malware protection.
- Implement additional custom validation rules for high-risk fields.

Limitation and Control of Network Ports, Protocols, and Services

Description: Manage (track, control, correct) the ongoing operational use of ports, protocols, and services on networked devices.
Status: Partially Implemented
Risk Rating: Medium
Details: Network ports, protocols, and services are monitored, but there are areas where control mechanisms need strengthening. Enhanced monitoring and automated tools are required to improve control.
Salesforce-Specific Findings:

- IP ranges for Salesforce access are not consistently enforced across all profiles.
- Some API endpoints are unnecessarily exposed.

Recommendations:

- Implement and enforce IP restrictions for all Salesforce profiles.
- Review and restrict API access to only necessary endpoints.
- Utilize Salesforce's Network Access feature to control access from specific IP ranges.
- Implement regular audits of enabled Salesforce features and APIs.

Data Recovery Capabilities

Description: Ensure that the organization has a data recovery capability that can restore the confidence in the integrity of the information system.
Status: Fully Implemented
Risk Rating: Low
Details: Comprehensive data recovery plans are in place, including regular backups and tested recovery procedures. These capabilities ensure that critical data can be restored quickly and accurately.
Salesforce-Specific Findings:

- Weekly data exports are performed and stored securely.
- Salesforce's Data Recovery service is available as a last resort.

Recommendations:

- Continue current practices.
- Implement Salesforce's Sandbox refresh feature for testing recovery procedures.
- Consider increasing the frequency of data exports to daily for critical data.

Secure Configuration for Network Devices

Description: Establish, implement, and actively manage the security configuration of network infrastructure devices.
Status: Partially Implemented
Risk Rating: Medium
Details: Secure configurations are applied to network devices, but improvements are needed in the consistency and comprehensiveness of these configurations. Regular reviews and updates are necessary.
Salesforce-Specific Findings:

- Salesforce connected apps are not consistently configured for secure access.
- Salesforce connected apps are not consistently configured for secure access.
- Some custom integrations lack proper security configurations.

Recommendations:

- Review and update security settings for all Salesforce connected apps.
- Implement stricter OAuth policies for custom integrations.
- Utilize Salesforce's Named Credentials feature for secure endpoint configurations.
- Conduct regular security reviews of all integrations and connected apps.

Boundary Defense

Description: Detect, prevent, and correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.
Status: Partially Implemented
Risk Rating: High
Details: Boundary defense mechanisms are in place, but there are gaps in monitoring and controlling data flow between different networks. Strengthening these defenses will improve overall security.
Salesforce-Specific Findings:

- Data loss prevention (DLP) measures are not fully implemented in Salesforce.
- Cross-org data sharing lacks proper security controls.

Recommendations:

- Implement Salesforce Shield Platform Encryption for sensitive data.
- Utilize Salesforce's Transaction Security policies to monitor and control data access.
- Implement stricter controls for cross-org data sharing, including proper authentication and authorization.
- Regularly review and update sharing rules and OWDs (Organization-Wide Defaults).

Data Protection

Description: Protect the organization's data through encryption, segmentation, and other means.
Status: Fully Implemented
Risk Rating: Low
Details: Data protection measures, including encryption and data segmentation, are fully implemented to safeguard sensitive information. These measures are regularly reviewed and updated.
Salesforce-Specific Findings:

- Field-level encryption is implemented for sensitive fields.
- Salesforce Shield Platform Encryption is used for data at rest.

Recommendations:

- Continue current practices.
- Regularly review and update field-level security settings.
- Consider implementing Salesforce's Event Monitoring for enhanced data access tracking.

Controlled Access Based on the Need to Know

Description: Enforce the principles of least privilege and separation of duties by restricting access to sensitive information based on need to know.
Status: Fully Implemented
Risk Rating: Low
Details: Access controls are enforced to ensure that users only have access to the information necessary for their roles. Regular audits are conducted to maintain these controls.
Salesforce-Specific Findings:

- Role hierarchy and sharing rules are properly configured.
- Field-level security is implemented for sensitive fields.

Recommendations:

- Continue regular audits of access controls.
- Implement Salesforce's Permission Set Groups for more granular access control.
- Regularly review and update sharing rules and role hierarchy.

Wireless Access Control

Description: Protect the organization's information by managing wireless access and its usage.
Status: Not Applicable
Risk Rating: Low
Details: This control is not applicable as wireless access management is handled outside of the Salesforce org.

Account Monitoring and Control

Description: Actively manage the lifecycle of system and application accounts, including their creation, use, and deletion.
Status: Partially Implemented
Risk Rating: High
Details: Account management processes are in place, but there are areas for improvement, particularly in monitoring and controlling privileged accounts.
Salesforce-Specific Findings:

- 15% of users have administrative privileges, which is higher than recommended.
- Multi-Factor Authentication (MFA) is only enabled for 60% of users.
- User access reviews are conducted annually, but best practice suggests quarterly reviews.

Recommendations:

- Implement stricter password policies (increase minimum length to 12 characters and require high complexity).
- Reduce session timeout to 1 hour for enhanced security.
- Enable MFA for all users, especially those with administrative privileges.
- Conduct quarterly user access reviews.
- Implement automated alerts for unusual account activities using Salesforce Event Monitoring.
- Utilize Salesforce Shield for enhanced monitoring capabilities.

Security Awareness and Training

Description: Implement a security awareness and training program to ensure that all users understand and comply with security policies.
Status: Partially Implemented
Risk Rating: Medium
Details: Security awareness training is conducted, but there is a need for more comprehensive and frequent training sessions. Enhanced training materials and regular updates are required.
Salesforce-Specific Findings:

- Basic Salesforce security training is provided during onboarding.
- No regular refresher courses on Salesforce security best practices.

Recommendations:

- Develop and implement more comprehensive Salesforce-specific security awareness training programs.
- Conduct quarterly training sessions on Salesforce security features and best practices.
- Implement simulated phishing exercises that include Salesforce-specific scenarios.
- Utilize Salesforce Trailhead modules for ongoing user education on security topics.

Application Software Security

Description: Manage the security lifecycle of all in-house developed and acquired software to prevent, detect, and correct security weaknesses.
Status: Partially Implemented
Risk Rating: High
Details: Security measures are in place for application software, but there are areas where improvements are needed. Regular code reviews and security testing will enhance this control.
Salesforce-Specific Findings:

- Custom Apex code is not consistently reviewed for security vulnerabilities.
- Third-party AppExchange applications are not regularly assessed for security risks.

Recommendations:

- Implement regular security code reviews for all custom Apex code.
- Conduct thorough security testing for all in-house developed Salesforce components.
- Establish a formal process for assessing and managing the security of AppExchange applications.
- Utilize Salesforce Security Scanner for automated code analysis.
- Implement Salesforce DevOps practices to ensure security is integrated into the development lifecycle.

Incident Response and Management

Description: Develop and implement incident response capabilities to quickly discover an attack, contain the damage, and restore normal operations.
Status: Fully Implemented
Risk Rating: Low
Details: Incident response plans are well-established and regularly tested. The organization is capable of quickly identifying, containing, and responding to security incidents.
Salesforce-Specific Findings:

- Incident response plan includes Salesforce-specific scenarios.
- Salesforce admin team is well-trained in incident response procedures.

Recommendations:

- Continue regular testing and updating of incident response plans.
- Conduct tabletop exercises that include Salesforce-specific security incidents.
- Implement automated alerting for potential security incidents using Salesforce Event Monitoring.
- Ensure that the incident response plan is updated to reflect new Salesforce features and potential vulnerabilities.

Penetration Tests and Red Team Exercises

Description: Test the overall strength of the organization's defense (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.
Status: Partially Implemented
Risk Rating: Medium
Details: Penetration tests are conducted periodically, but there is a need for more frequent and comprehensive testing. Red team exercises will further enhance the organization's security posture.
Salesforce-Specific Findings:

- Salesforce org is included in annual penetration tests.
- No Salesforce-specific red team exercises have been conducted.

Recommendations:

- Conduct Salesforce-specific penetration tests semi-annually.
- Implement red team exercises that include scenarios targeting Salesforce data and configurations.
- Utilize Salesforce's Sandbox environments for security testing and simulations.
- Engage Salesforce security specialists for targeted assessments of custom developments and configurations.

10 Implementation Roadmap

To address the identified gaps and improve the overall security posture of our Salesforce org, we propose the following implementation roadmap:

Timeline	Action Item	Priority	Status
Q3 2024	Enable MFA for all users	High	Planned
Q3 2024	Implement stricter password policies	High	Planned
Q3 2024	Reduce admin privileges to ¡5% of users	High	Planned
Q4 2024	Implement Salesforce Shield	Medium	Planned
Q4 2024	Conduct Salesforce-specific security training	Medium	Planned
Q1 2025	Implement automated code review process	Medium	Not Started
Q1 2025	Conduct Salesforce-specific penetration test	High	Not Started
Q2 2025	Implement Salesforce DevOps practices	Low	Not Started

11 Conclusion

This gap assessment has identified several areas where our current security controls in Salesforce do not fully align with the CIS Controls framework. By implementing the recommended measures, we can significantly enhance our Salesforce security posture and better protect our sensitive data.

12 Appendices

Appendix A: Salesforce Security Features

- Multi-Factor Authentication (MFA)
- Field-Level Security
- Sharing Rules and Organization-Wide Defaults (OWD)
- Salesforce Shield (Platform Encryption, Event Monitoring, Field Audit Trail)
- Login IP Ranges
- Session Security Settings

Appendix B: Relevant Salesforce Compliance Standards

- SOC 2
- ISO 27001

- HIPAA (for Healthcare organizations)
- GDPR (for organizations handling EU citizen data)

13 References

- CIS Controls v8
- Salesforce Security Guide
- NIST SP 800-53 Rev. 5
- Salesforce Administrator Guide
- Salesforce Platform Developer Guide
- Salesforce Shield Implementation Guide
- OWASP Top 10 for Salesforce

14 Glossary

CIS Center for Internet Security

MFA Multi-Factor Authentication

API Application Programming Interface

DLP Data Loss Prevention

OWD Organization-Wide Defaults

SOQL Salesforce Object Query Language

SOSL Salesforce Object Search Language

TLS Transport Layer Security

SSO Single Sign-On

15 Document Revision History

Version	Date	Description of Changes	Author
1.0	08/07/2024	Initial document creation	A. Anthony
1.1	08/07/2024	Updated with Salesforce-specific details	A. Anthony

16 Approval

This document has been reviewed and approved by:

Name: **Signature:**

Title: **Date:**

Name: **Signature:**

Title: **Date:**

17 Disclaimer

This gap assessment report is based on information available at the time of the assessment and may not reflect all potential vulnerabilities or risks. It is recommended to regularly review and update security measures as new threats emerge and technology evolves.

18 Contact Information

For any questions or clarifications regarding this report, please contact:

Name:	Anderson Anthony
Title:	Chief Compliance Officer
Email:	Anderson@cloudstrategik.com
Phone:	+1 (555) 123-4567