# Salesforce Security Operational Playbook



## **Contents**

- 3 Introduction
- 4 Development Cycle
- 4 Requirements
- 5 Development
- 6 Quality Assurance
- 7 User Acceptance Testing (UAT)
- 8 Release
- 9 Sales Reporting Cycle
- 9 Weekly
- 9 Monthly
- 10 Quarterly
- 10 Support
- 11 About Own

#### Jump to:

#### **Development Cycle**

- Requirements
- Development
- Quality Assurance
- User Acceptance Testing
- Release

### **Security Reporting Cycle**

- Weekly
- Monthly
- Quarterly
- Support



### Introduction

To operationalize your Salesforce Security
Operating Model leveraging Own's Secure®,
we recommend the following steps. They are broken
down into two sections: The first, integration with
the Development Cycle, and second, integration
into a Security Reporting Cycle.

We suggest that customers engage the appropriate constituents for a working session to discuss the unique processes of their organization and create a strategy and definition for their own enterprise-specific Security Operating Model.

NOTE: Own offers onboarding workshops to support customers through this process as needed.

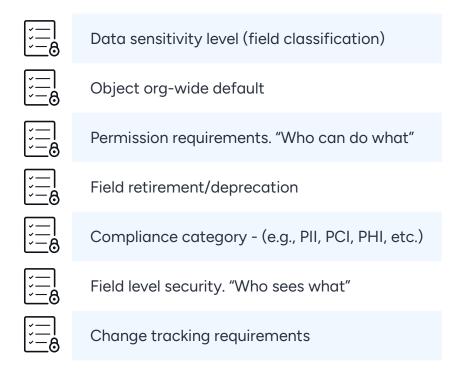


# Requirements

**Environment:** Document **Secure Module:** N/A

Roles Involved: Architect, Business Analyst, Security Analyst.

Develop feature security requirements including where applicable:





## Development

**Environment: Development** 

Secure Module: Data Classification, Platform Encryption, Analyzer,

History Retention Policy Roles Involved: Developer

Develop/configure to business and security requirements:

### Own Secure®



Fields configured for encryption and compliancecategorization)



Encryption blockers identified and removed



Field usage set for deprecated fields (hidden, deprecatecandidate, active)



Change tracking/history retention policies configured



Compliance category (e.g., PII, PCI, PHI, etc.)

### Salesforce setup



Field level security configured



Permissions configured (profile or permission sets updated)



Object org-wide default configured



## **Quality Assurance**

**Environment:** QA/Regression

Secure Module: Data Classification, Platform Encryption Analyzer,

History Retention Policy, Who Sees What Explorer

Roles Involved: QA

Validate development/configuration/deployment of security requirements:

### Own Secure®



Confirm field classification



Confirm compliance categorization



Removal of access to deprecated fields



Confirm field usage



Confirm field level security



Confirm change tracking

### Salesforce setup



Confirm deprecated fields removed from layouts



Confirm deprecated fields removed (if possible) & data migrated



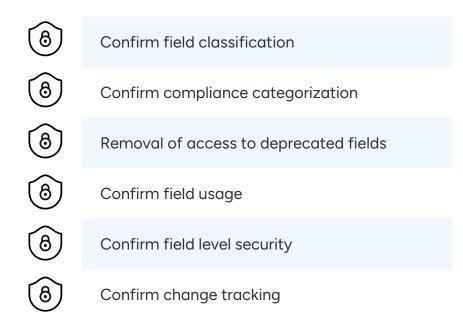
# User Acceptance Testing (UAT)

**Environment: UAT** 

Secure Module: Data Classification, Platform Encryption Analyzer,

History Retention Policy, Who Sees What Explorer **Roles Involved:** Business Analyst, Salesforce Admin

Validate development/configuration/deployment of security requirements:



### Salesforce setup







### Release

**Environment:** Production

Secure Module: Data Classification, Platform Encryption Analyzer,

History Retention Policy, Who Sees What Explorer **Roles Involved:** Security Analyst, Salesforce Admin

Validate development/configuration/deployment of security requirements:

### Own Secure®



Confirm compliance categorization

Removal of access to deprecated fields

Confirm field usage

Confirm field level security

Confirm change tracking

### Salesforce setup

Confirm deprecated fields removed from layouts

Confirm deprecated fields removed (if possible) & data migrated



## Weekly

**Environment: Production** 

Secure Module: Data Classification

Roles Involved: Security Analyst, Salesforce Admin

Identify new unclassified fields in org

If new fields, classify them

Determine field usage for new, unused fields

Create requirements to remove access via field level security, remove from layouts

# Monthly

**Environment:** Production

Secure Module: Platform Encryption Analyzer, Security Insights

Roles Involved: Security Analyst, Salesforce Admin

Identify new configuration blockers to encrypted

Create requirements to remediate

Look for decreased scores in Security Insights dashboard, investigate reasons why

Create requirements to remove access via field level security, remove from layouts



## Quarterly

**Environment: Production** 

Secure Module: Security Insights

Roles Involved: Security Analyst, Salesforce Admin

Compare scores from last quarter, identify reasons

for lower scores

Create requirements to remediate if required

## Support

**Environment: Production** 

Secure Module: Who Sees What Explorer, Security Access Explorer

Roles Involved: Salesforce Support

Troubleshoot field level security issues





### OWN YOUR OWN DATA

### **About Own**

Own is the leading data platform trusted by thousands of organizations to protect and activate SaaS data to transform their businesses. Own empowers customers to ensure the availability, security and compliance of mission-critical data, while unlocking new ways to gain deeper insights faster. By partnering with some of the world's largest SaaS ecosystems such as Salesforce, ServiceNow and Microsoft Dynamics 365, Own enables customers around the world to truly own the data that powers their business.

lt's their platform. It's your data. Own it

Learn more at owndata.com