REVCULT'S

Salesforce Security Operational Playbook

RevCult

To operationalize your Salesforce Security Operating Model leveraging Cloud Security Cockpit® (“CSC”), RevCult recommends 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: *RevCult offers onboarding workshops to support customers through this process as needed.*

Jump To:

DEVELOPMENT CYCLE

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

SECURITY REPORTING CYCLE

- **Weekly**
- **Monthly**
- **Quarterly**
- **Support**

Requirements

1

ENVIRONMENT: Document

CSC MODULE: N/A

ROLES INVOLVED: Architect,Business Analyst, Security Analyst

DEVELOP FEATURE SECURITY REQUIREMENTS INCLUDING WHERE APPLICABLE:

- **Data sensitivity level (field classification)**
- **Compliance category (e.g., PII, PCI, PHI, etc.)**
- **Object org-wide default**
- **Field level security "Who sees what"**
- **Permission requirements "Who can do what"**
- **Change tracking requirements**
- **Field retirement/ deprecation**

Development 2

ENVIRONMENT: Development

CSC MODULE: Data Classification, Platform Encryption Analyzer, History Retention Policy

ROLES INVOLVED: Developer

DEVELOP/CONFIGURE TO BUSINESS AND SECURITY REQUIREMENTS.

Cloud Security Cockpit®

- Fields configured for encryption and compliance categorization
- Field usage set for deprecated fields (hidden, deprecate candidate, active)
- Encryption blockers identified and removed
- Change tracking / history retention policies configured

Salesforce Setup

- Field level security configured
- Object org-wide default configured
- Permissions configured (profile or permission sets updated)

Quality Assurance

3

ENVIRONMENT: QA / Regression

CSC MODULE: Data Classification, Platform Encryption Analyzer, History Retention Policy, Who Sees What Explorer

ROLES INVOLVED: QA

VALIDATE DEVELOPMENT/CONFIGURATION/DEPLOYMENT OF SECURITY REQUIREMENTS

Cloud Security Cockpit®

Confirm field classification

Confirm field usage

Confirm compliance categorization

Confirm field level security

Removal of access to deprecated fields

Confirm change tracking

Salesforce Setup

Confirm deprecated fields removed from layouts

Confirm deprecated fields removed (if possible) & data migrated

User Acceptance Testing (UAT)

4

ENVIRONMENT: UAT

CSC MODULE: Data Classification, Platform Encryption Analyzer, History Retention Policy, Who Sees What Explorer

ROLES INVOLVED: Business Analyst, SF Admin

VALIDATE DEVELOPMENT/CONFIGURATION/DEPLOYMENT OF SECURITY REQUIREMENTS

Cloud Security Cockpit®

- Confirm field classification
- Confirm field usage
- Confirm compliance categorization
- Confirm field level security
- Removal of access to deprecated fields
- Confirm change tracking

Salesforce Setup

- Confirm deprecated fields removed from layouts
- Confirm deprecated fields removed (if possible) & data migrated

Release 5

ENVIRONMENT: Production

CSC MODULE: Data Classification, Platform Encryption Analyzer, History Retention Policy, Who Sees What Explorer

ROLES INVOLVED: Security Analyst, SF Admin

VALIDATE DEVELOPMENT/CONFIGURATION/DEPLOYMENT OF SECURITY REQUIREMENTS

Cloud Security Cockpit®

Confirm field classification

Confirm field usage

Confirm compliance categorization

Confirm field level security

Removal of access to deprecated fields

Confirm change tracking

Salesforce Setup

Confirm deprecated fields removed from layouts

Confirm deprecated fields removed (if possible) & data migrated

Weekly

ENVIRONMENT: Production
CSC MODULE: Data Classification
ROLES INVOLVED: Security Analyst, SF 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
CSC MODULE: Platform Encryption Analyzer, Security Insights
ROLES INVOLVED: Security Analyst, SF Admin

- **Identify new configuration blockers to encrypted Fields**
  - **Create requirements to remediate**
- **Look for decreased scores in Security Insights dashboard, investigate reasons why**
  - **Create requirements to remediate if required**

Quarterly

ENVIRONMENT: Production
CSC MODULE: Security Insights
ROLES INVOLVED: Infosec, Audit

- **Compare scores from last quarter, identify reasons for lower scores**
- **Create requirements to remediate if required**

Support

ENVIRONMENT: Production
CSC MODULE: Who Sees What Explorer, Security Access Explorer
ROLES INVOLVED: SF Support

- **Troubleshoot field level security issues**

Any Questions? Please contact us at **revcult.com/contact-us**