APPROVED

SOP-004 v1.0 – Change Control for VDC

Approver
2026-01-30 00:55:19

Document ID: SOP-004
Title: Change Control for VDC
Version: v1.0
Effective Date: January 29, 2026
Owner: VDC System Owner: William O'Connell
Approved By: QA / Compliance Lead: Jane Smith

---

1. Purpose

The purpose of this SOP is to define the change control process for the Validated Document Control (VDC) system hosted at https://williamoconnellpmp.com. This SOP ensures that all changes to the system are properly evaluated, approved, tested, and documented to maintain the validated state and GxP compliance.

---

2. Scope

This SOP applies to:

- All changes to the VDC production environment, including:
  - Code changes (Lambda functions, frontend application)
  - Infrastructure changes (CloudFormation templates, AWS resource configurations)
  - Configuration changes (Cognito settings, DynamoDB schema, S3 bucket policies)
  - Documentation changes (SOPs, validation documents, user guides)
- All personnel involved in proposing, reviewing, approving, implementing, or testing changes
- Emergency changes requiring expedited approval

This SOP does not cover:

- Changes to development/test environments (unless they affect production validation)
- Routine operational activities defined in other SOPs (e.g., user provisioning per SOP-002)

---

3. Definitions

- **Change:** Any modification to the VDC system that could affect functionality, performance, security, compliance, or validation status.
- **Change Request (CR):** Formal documentation proposing a change, including justification, impact assessment, and implementation plan.
- **Emergency Change:** A change required to address a critical system failure, security vulnerability, or regulatory non-compliance that cannot wait for standard approval cycle.
- **Impact Assessment:** Evaluation of how a change affects system functionality, GxP compliance, validation status, and related systems.
- **Regression Testing:** Testing to verify that existing validated functionality still works correctly after a change.
- **Revalidation:** Partial or full validation activities required when a change significantly affects validated functionality.

---

4. Roles and Responsibilities

APPROVED

Approver
2026-01-30 00:55:19

System Owner

- Reviews and approves all non-emergency change requests
- Determines if a change requires revalidation
- Ensures adequate resources for change implementation and testing

QA / Compliance

- Reviews impact assessments for GxP and regulatory implications
- Approves changes affecting validated functionality
- Determines scope of regression testing and revalidation
- Reviews test results before change closure

Change Originator

- Submits change request with complete justification and impact assessment
- Provides technical details and implementation plan
- May be: Developer, System Administrator, End User, or External Auditor

System Administrator / Developer

- Implements approved changes per approved implementation plan
- Executes testing per test protocols
- Documents change execution and results
- Performs rollback if necessary

End Users

- May initiate change requests for functionality enhancements or issue resolution
- Participate in User Acceptance Testing (UAT) when applicable

---

5. Change Classification

All changes must be classified into one of the following categories:

5.1 Category 1: Minor Changes (Low Impact)

Definition: Changes with minimal or no impact on validated functionality, GxP compliance, or system performance.

Examples: - Cosmetic UI changes (color, font size, layout) that do not affect workflow - Documentation updates (typo fixes, clarifications) - Addition of non-GxP reporting or analytics features - Infrastructure scaling (e.g., increasing DynamoDB capacity) without functional changes

Approval Required: - System Owner approval only - QA notification (no formal approval needed)

Testing Required: - Smoke testing to verify no unintended side effects - No formal regression testing required

Revalidation Required: No

5.2 Category 2: Moderate Changes (Medium Impact)

Definition: Changes that modify validated functionality but do not alter core GxP processes or introduce new regulatory requirements.

Examples: - Adding new non-critical fields to document metadata - Performance optimizations (e.g., Lambda timeout adjustments, API Gateway caching) - Changes to error messages or user notifications - Addition of new user roles (beyond Submitter/Approver) - Updates to AWS service versions (e.g., Lambda runtime upgrades)

Approval Required: - System Owner approval - QA / Compliance approval

Testing Required: - Functional testing of changed components - Targeted regression testing of related functionality - Test protocol documented and results reviewed

Revalidation Required: Partial (affected requirements only)

APPROVED

Approver

2026-01-30 00:55:19

5.3 Category 3: Major Changes (High Impact)

Definition: Changes that significantly alter validated functionality, introduce new GxP-critical features, or modify audit trail, security, or electronic signature capabilities.

Examples: - Changes to approval workflow logic (e.g., multi-level approvals) - Modifications to audit trail capture or storage - Changes to authentication/authorization mechanisms (e.g., replacing Cognito) - New document types or lifecycle states - Database schema changes affecting validated data - Migration to new AWS regions or accounts - Integration with external systems (e.g., ERP, LIMS)

Approval Required: - System Owner approval - QA / Compliance approval - Additional stakeholder approval (e.g., Business Process Owner) if applicable

Testing Required: - Complete regression testing per RTM - Performance Qualification (PQ) for affected workflows - Test protocols must be pre-approved by QA

Revalidation Required: Yes (formal IQ/OQ/PQ or equivalent)

5.4 Emergency Changes

Definition: Changes required to address critical system failures, security vulnerabilities, or regulatory non-compliance that pose immediate risk.

Examples: - Critical security patches (e.g., CVE vulnerabilities in dependencies) - System outage requiring immediate infrastructure changes - Data integrity issues requiring immediate remediation - Regulatory findings requiring urgent corrective action

Approval Required: - Verbal approval from System Owner and QA (documented within 24 hours) - Formal Change Request submitted retrospectively within 48 hours

Testing Required: - Pre-implementation testing in non-production environment if possible - Post-implementation verification in production - Full regression testing within 5 business days

Revalidation Required: Determined by QA within 48 hours of implementation

---

6. Change Control Process

6.1 Change Initiation

1. Change Originator completes Change Request (CR) form including:
   - CR ID (sequential number: CR-YYYY-NNN)
   - Change title and description
   - Business justification and benefits
   - Proposed change classification (Category 1/2/3)
   - Affected system components (Lambda functions, DynamoDB tables, S3 buckets, etc.)
   - Impact assessment (see Section 6.2)
   - Implementation plan with timeline
   - Rollback plan
   - Testing approach

2. Submit CR to System Owner via approved mechanism (ticketing system, email, or change request log)

APPROVED

Approver

2026-01-30 00:55:19

6.2 Impact Assessment

Change Originator must evaluate and document impact in the following areas:

Functional Impact

- Does the change affect document submission, approval, or retrieval workflows?
- Are new features being added or existing features modified?
- Will user experience change?

GxP / Regulatory Impact

- Does the change affect 21 CFR Part 11 compliance (audit trail, e-signatures, access controls)?
- Are ALCOA+ principles maintained (Attributable, Legible, Contemporaneous, Original, Accurate)?
- Does the change affect validated functionality documented in URS/FS?

Data Integrity Impact

- Will existing data need to be migrated or transformed?
- Are audit records affected?
- Is data encryption or access control changing?

Performance Impact

- Will the change affect system response time or throughput?
- Are new resource limits (Lambda timeout, DynamoDB capacity) required?

Security Impact

- Does the change introduce new attack surfaces?
- Are IAM policies or security groups being modified?
- Is authentication or authorization logic changing?

Integration Impact

- Are other systems or external services affected?
- Will APIs or data interfaces change?

Validation Impact

- Which URS requirements are affected? (Reference URS requirement IDs)
- Which test cases need to be re-executed? (Reference RTM)
- Is revalidation required?

6.3 Change Review and Approval

Category 1 (Minor) Changes

1. System Owner reviews CR and impact assessment
2. System Owner approves or rejects with comments
3. QA is notified (CC’d on approval) but formal approval not required
4. If approved, proceed to Section 6.4 (Implementation)

Category 2 (Moderate) Changes

1. System Owner reviews CR and impact assessment
2. System Owner provides preliminary approval or requests modifications

3. QA / Compliance reviews for regulatory impact
4. QA / Compliance approves or rejects with comments
5. If approved by both, proceed to Section 6.4 (Implementation)

Category 3 (Major) Changes

1. System Owner reviews CR and impact assessment
2. System Owner provides preliminary approval or requests modifications
3. QA / Compliance conducts detailed validation impact assessment
4. Test protocols prepared and submitted to QA for pre-approval
5. Additional stakeholders review if needed (Business Process Owner, IT Security)
6. Formal approval meeting with documented decision
7. If approved, proceed to Section 6.4 (Implementation)

Emergency Changes

1. System Owner and QA provide verbal approval (phone, video call)
2. Verbal approval documented in change log within 24 hours
3. Change implemented immediately
4. Formal CR submitted retrospectively within 48 hours
5. QA determines revalidation scope within 48 hours
6. Follow-up review conducted within 5 business days

6.4 Change Implementation

1. **Pre-Implementation:**
   - System Administrator/Developer reviews approved CR and implementation plan
   - Backup of current production state performed per SOP-008
   - Change scheduled during approved maintenance window (or immediately for emergency changes)
   - Stakeholders notified of planned downtime if applicable
2. **Implementation:**
   - Developer implements change per approved plan
   - All steps documented (Git commits, CloudFormation stack updates, AWS console actions)
   - Implementation evidence captured (screenshots, logs, command output)
   - Rollback plan kept readily available
3. **Post-Implementation:**
   - Developer executes smoke tests to verify basic functionality
   - System Administrator verifies all AWS resources deployed correctly
   - No errors in CloudWatch Logs for critical Lambda functions

---

6.5 Change Testing

Testing must be performed according to change classification:

Category 1 Testing

- Smoke testing: Verify login, document list loads, no console errors
- Visual inspection of changed UI elements
- No formal test protocol required
- Test results documented in CR comments

Category 2 Testing

- Functional testing of changed components per written test cases
- Targeted regression testing of related functionality (e.g., if upload changes, test submit workflow)
- Test protocol with expected/actual results
- QA reviews test results before change closure

Category 3 Testing

- Full regression testing per RTM (all affected URS requirements)
- Performance Qualification (PQ) for affected workflows

- Test protocols pre-approved by QA
- Formal test execution with screenshots/evidence
- QA approves test results before production deployment

Emergency Change Testing

- Pre-implementation testing in DEV environment if possible (time permitting)
- Post-implementation verification in production (smoke tests)
- Full regression testing within 5 business days
- Compensating controls documented if full testing delayed

6.6 Change Closure

1. Developer updates CR with:
    - Implementation completion date/time
    - Test results summary (or link to test protocol)
    - Any deviations from approved plan
    - Actual vs. planned effort
2. QA reviews:
    - Test results meet acceptance criteria
    - Validation status confirmed (no revalidation needed, or revalidation completed)
    - No unresolved deviations
3. System Owner reviews:
    - Change objectives achieved
    - No adverse business impact
    - System performance acceptable
4. CR marked as **Closed** with final approval signatures
5. Change documented in Change Control Log (see Section 7)

6.7 Rollback Procedures

If a change causes unexpected issues, rollback must be initiated:

Trigger Conditions for Rollback: - Critical functionality broken (cannot submit/approve documents) - Data integrity issue detected (audit trail not recording, hash calculation failing) - Security vulnerability introduced - Performance degradation beyond acceptable thresholds - QA / System Owner determination

Rollback Process: 1. System Owner or QA authorizes rollback (verbal approval acceptable) 2. Developer executes rollback plan: - Revert CloudFormation stack to previous version - Restore Lambda function code from previous deployment - Restore DynamoDB tables from Point-in-Time Recovery if needed (per SOP-008) - Revert S3 bucket configurations 3. Smoke testing performed to verify rollback successful 4. Root cause analysis initiated per SOP-005 (Deviation/CAPA) 5. CR updated with rollback details and marked as **Rolled Back** 6. New CR required to re-attempt change after issue resolution

---

7. Change Control Log

A Change Control Log must be maintained with the following information for all CRs:

Field	Description
CR ID	Unique sequential identifier (CR-2026-001)
Title	Brief description of change
Classification	Category 1, 2, 3, or Emergency
	Name and email of person requesting

APPROVED

Approver

2026-01-30 00:55:19

Originator	change
Submission Date	Date CR submitted
Approval Date	Date CR approved (or rejected)
Implementation Date	Date change deployed to production
Affected Components	Lambda functions, DynamoDB tables, S3 buckets, etc.
URS Requirements Affected	List of URS requirement IDs
Test Protocol ID	Reference to test documentation
Status	Draft, Pending Approval, Approved, Implemented, Closed, Rejected, Rolled Back
Approvers	System Owner, QA, additional approvers
Closure Date	Date CR formally closed

Log Location: Change Control Log maintained in controlled repository (e.g., SharePoint, Git repository, ticketing system)

Retention: Change Control Log retained per SOP-008 (minimum 7 years)

---

8. Annual Change Control Review

At least annually (or more frequently if change volume is high), System Owner and QA conduct a Change Control Review:

Review Objectives: - Assess effectiveness of change control process - Identify trends (common change types, frequent issues) - Verify all changes properly classified and approved - Confirm no unauthorized changes occurred - Review rollback incidents and root causes - Identify process improvements

Review Deliverable: - Change Control Annual Review Report including: - Total number of changes by category - Average time from submission to closure - Number of rollbacks and reasons - Validation impact summary (how many changes required revalidation) - Process improvement recommendations

Review results discussed with stakeholders and action items tracked per SOP-005 (CAPA)

---

9. Integration with Other SOPs

This SOP integrates with:

- **SOP-001 (System Governance):** Changes must maintain validated state defined in Section 9 (Periodic Review and Revalidation)
- **SOP-002 (User Management):** Role changes follow this change control process per Section 7
- **SOP-004 (Document Lifecycle):** Workflow changes require Category 3 change control
- **SOP-005 (Deviation/CAPA):** Rollbacks or change-related issues generate deviations
- **SOP-008 (Backup/Retention):** Pre-implementation backups required before major changes

---

10. References

- 21 CFR Part 11, Electronic Records; Electronic Signatures
- GAMP 5, “A Risk-Based Approach to Compliant GxP Computerized Systems” (Chapter 5: Change Control)
- ICH Q9, Quality Risk Management
- Internal quality policies on change control and validation

APPROVED

Approver

2026-01-30 00:55:19

11. Revision History

Version	Date	Author	Description of Changes
1.0	Jan 29, 2026	William O’Connell	Initial release

12. Approval

System Owner:
William O’Connell
January 29, 2026

QA / Compliance Lead:
Jane Smith
January 29, 2026