

Template

StateRAMP Configuration management Plan

(CMP)

Service Provider Name

Information System Name

**VERSION:**

X.X

**DATE:**

YYYYMMDD

Executive Summary

This document supports configuration management requirements for the State Risk and Authorization Management Program (StateRAMP) and contains the CMP for {Information System Name}. A CMP describes the measures for establishing the configuration baseline and managing configurations for all information system components. It also describes the change management process and the security considerations that are built into the process to ensure secure configurations are maintained. These configurations and change management efforts are integral to managing security risks for the information system.

System Security Plan

Prepared by

|  |
| --- |
| **Identification of Organization that Prepared this Document** |
|  | Organization Name | <Enter Company/Organization>. |
| Street Address | <Enter Street Address> |
| Suite/Room/Building | <Enter Suite/Room/Building> |
| City, State Zip | <Enter Zip Code> |

Prepared for

|  |
| --- |
| Identification of Cloud Service Provider |
|  | Organization Name | <Enter Company/Organization>. |
| Street Address | <Enter Street Address> |
| Suite/Room/Building | <Enter Suite/Room/Building> |
| City, State Zip | <Enter Zip Code> |

Template Revision History

| Date | Description |
| --- | --- |
| 4/6/2021 | Original publication |

Document Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Description | Version of CMP | Author |
| <Date> | <Revision Description> | <Version> | <Author> |
| <Date> | <Revision Description> | <Version> | <Author> |
| <Date> | <Revision Description> | <Version> | <Author> |

How to contact us

For questions about StateRAMP, or for technical questions about this document including how to use it, contact pmo@StateRAMP.org. For more information about the StateRAMP project, see [www.StateRAMP.org](https://www.stateramp.org/)

TABLE OF CONTENTS

[1. Introduction & Purpose 5](#_Toc71708504)

[2. Scope 5](#_Toc71708505)

[3. System Description 5](#_Toc71708506)

[3.1 System Development Life Cycle (SDLC) 5](#_Toc71708507)

[4. Configuration Management Policy 6](#_Toc71708508)

[5. Roles and Responsibilities 6](#_Toc71708509)

[6. Configuration Control Board 6](#_Toc71708510)

[7. Baseline Configuration Management 6](#_Toc71708511)

[8. Requesting a Change 6](#_Toc71708512)

[8.1 Change Types and Schedules 6](#_Toc71708513)

[8.2 Change Planning 7](#_Toc71708514)

[8.3 Change Testing and Security Impact Analysis 7](#_Toc71708515)

[8.4 Change Implementation 7](#_Toc71708516)

[8.5 Change Control and Documentation 8](#_Toc71708517)

[8.6 Change Monitoring 8](#_Toc71708518)

[8.7 Communication and Reporting of Changes 8](#_Toc71708519)

[8.8 Maintenance Window 8](#_Toc71708520)

[9. Appendix A: Change Request Form 9](#_Toc71708521)

[10. Appendix B: Security Impact Analysis 10](#_Toc71708522)

List of Tables

[Table 1‑1. Information System Name and Title 5](#_Toc71708523)

[Table 2‑3. Roles and Responsibilities 6](#_Toc71708524)

[Table 8‑2. Cloud Deployment Model Represented in this SSP 7](#_Toc71708525)

Configuration Management Plan Approvals

Cloud Service Provider Signatures

|  |
| --- |
|  |
| Name | <Enter Name> | Date | <Select Date> |
| Title | <Enter Title> |
| Cloud Service Provider | CSP Name |
|  |
|  |
|  |
| Name | <Enter Name> | Date | <Select Date> |
| Title | <Enter Title> |
| Cloud Service Provider | CSP Name |
|  |
|  |
|  |
| Name | <Enter Name> | Date | <Select Date> |
| Title | <Enter Title> |
| Cloud Service Provider | CSP Name |
|  |  |

# Introduction & Purpose

Information systems are vital to {company name} mission/business functions; therefore, it is critical that the information system components are securely configured and that all changes to the system are strictly controlled. This CMP describes the comprehensive procedures used to establish secure configurations and subsequently coordinate, manage, control, test, implement, and validate all changes to the system. An information system is typically in a constant state of change in response to new, enhanced, corrected, or updated hardware and software capabilities, patches for correcting software flaws, and other errors to existing components, new security threats, changing business functions, etc.

Implementing information system changes almost always results in some adjustment to the system configuration. To ensure that the required adjustments to the system configuration do not adversely affect the security of the information system or the organization from operation of the information system, a well-defined configuration management process that integrates information security is needed. One of the goals of a CMP is to manage and monitor the configurations of information systems to achieve adequate security and minimize organizational risk while supporting the desired business functionality and services. This includes configuration management activities at both the organizational and system levels.

| Unique Identifier | Information System Name | Information System Abbreviation |
| --- | --- | --- |
| Enter StateRAMP Package ID | Enter Information System Name | Enter Information System Abbreviation |

Table 1‑1. Information System Name and Title

# Scope

This CMP has been developed for {System Name}, which is classified as a {Category 1, 2, 3} system, in Section 15 of the StateRAMP SSP Data classification tool. The procedures in this CMP have been developed for a {Category 1, 2, 3} system and are designed to ensure control over any changes made to the system.

This CMP does not include customer responsibilities, which are listed below:

* {List Customer Responsibilities}

# System Description

{Insert from SSP}

## System Development Life Cycle (SDLC)

{Document Steps of SDLC or Reference related document}

# Configuration Management Policy

{Company Name}’s configuration management policy can be found in SSP\_A\_POL as {Insert Filename}.

# Roles and Responsibilities

{Company Name} establishes multiple roles and responsibilities to establish secure configurations and subsequently coordinate, manage, control, test, implement, and validate all changes to the information system.

| Role | Responsibilities |
| --- | --- |
| Change Management Users | * Creation of change request tickets
* Peer review of change
 |
| Change Approver (CAB) | * Approve or deny a change to information system
 |
| Change Manager | * Provides oversight of CAB meetings to ensure accuracy and completeness in accordance with change control process
 |
| Configuration Management User | * Have access to the configuration items in change management system
 |

Table 2‑3. Roles and Responsibilities

# Configuration Control Board

Insert how the board functions, its members, frequency of meetings, process for Change approvals. Delete this and all other instructions from your final version of this document.

# Baseline Configuration Management

Insert how you are managing baseline configuration for systems in your environment (System type, process for changes to baseline, images, software, etc. Delete this and all other instructions from your final version of this document.

# Requesting a Change

## Change Types and Schedules

Information systems are made up of different deployment models. The deployment models of the Enter Information System Abbreviation that are defined in this SSP and are not leveraged by any other StateRAMP Authorizations, are indicated in Table 8‑2 Cloud Deployment Model Represented in this SSP that follows.

Check deployment model that applies. Delete this and all other instructions from your final version of this document.

|  |  |  |
| --- | --- | --- |
| Change Type | Timeline | Required Approvals |
| Normal | 1-2 weeks | CAB (2/3s voting approval)  |
| Expedited | Less 1 week | Any one member of the CAB |
| Emergency | Immediate/same day | Approval or review after implementation by the CAB |
| Routine | Ongoing and new entries added to change schedule | CAB |

Table 8‑2. Cloud Deployment Model Represented in this SSP

## Change Planning

Planning considers if the requested change is appropriate for the environment, is it necessary, who it will impact, when will it be completed, what is the desired outcome, what constitutes a successful change, who needs to approve the change, and will other plans such as Disaster Recovery or Incident Response Management require updating based on this change.

This is the examples of phases for a change request. Delete this and all other instructions from your final version of this document.

1. Summary
2. Planning
3. Impact
4. Schedule
5. Assessment
6. Authorize
7. Schedule
8. Implement
9. Review
10. Close/cancel

## Change Testing and Security Impact Analysis

Document steps required for testing proposed changes, document process for conducting security impact analysis. Delete this and all other instructions from your final version of this document.

## Change Implementation

Document how changes are implemented, how review of completed changes is conducted (Peer review, Infrastructure as code review, etc.) Delete this and all other instructions from your final version of this document.

## Change Control and Documentation

Document required change control documentation (Phases of change, approvals, testing and implementation plan) Delete this and all other instructions from your final version of this document.

## Change Monitoring

Document how changes to systems are monitored (File integrity monitoring, Inventory Scanning, Code review). Delete this and all other instructions from your final version of this document.

## Communication and Reporting of Changes

Document how changes are communicated and to whom they are communicated to (System admins alerted of change via email, product features or functionality changes in web application provided to client via email/product update page, etc.). Delete this and all other instructions from your final version of this document.

## Maintenance Window

Document (if applicable) maintenance window for systems, include days and times normal system maintenance is conducted for production environments. Delete this and all other instructions from your final version of this document.

# Appendix A: Change Request Form

Insert relevant fields or examples of required change request form content. Delete this and all other instructions from your final version of this document.

# Appendix B: Security Impact Analysis

Insert relevant fields or examples of required change request form content. Delete this and all other instructions from your final version of this document.