State of California

California Department of Technology

Office of Technology Services

California Cloud Services Assessment Guide

SIMM 141

October 2023

REVISION HISTORY

REVISION	DATE OF RELEASE	OWNER	SUMMARY OF CHANGES
Initial Release	October 2023	Office of Technology Services	New process for California Cloud Services Assessment.

TABLE OF CONTENTS

I. Introduction

The Cloud Services Assessment Guide (Guide) provides instructions to submit California Cloud Services Assessment (CCSA) requests. The Guide is supplemental to the Off Premises Cloud Service request in the California Department of Technology (CDT) Information Technology (IT) Service Portal.

In accordance with Technology Letter (TL) 23-03, the Update to Cloud Computing Policy – Cloud Smart, and State Administrative Manual (SAM) 4983.1 Cloud Computing Policy, CDT will perform assessments to validate cloud design, workforce, procurement, and security requirements. This process is applicable to Agencies and/or state entities that plan to either introduce new systems or modify and migrate existing systems into the cloud. The assessment scope extends to both commercial and government cloud third-party providers and is at the system level. An assessment is required for each system in the cloud.

II. California Cloud Services Assessment (CCSA) Review Requirements

CCSA requests will be submitted in the CDT IT Service Portal accessed from the CDT Off-Premises Cloud Services website.

Once the request is complete, including all required documentation, a review will be initiated. The review is expected to take 14 business days. If documentation is missing or inadequate your Agency/state entity may be contacted for additional information which may extend the review time.

Documentation will be submitted through the CDT Secure Automated File Exchange (SAFE) account.

To ensure secure environments and proper utilization of cloud services, CDT reserves the right to perform health checks and audits on existing and new infrastructure services.

Below are requirements to complete the CCSA process.

1. Review the CDT CCSA website content including all the tabs to become familiar with the Cloud Computing request process.

    - All the templates and required documentation must be completed and prepared prior to creating a service request in the CDT Service Portal. The complete list of CDT templates and required documentation can be found on the California Cloud Services Assessment website under the “**Required Documentation Tab**”.

NOTE: The CDT Service Portal will time out in 15 minutes.

2. If the required documentation is not submitted or is incomplete, the service request will be closed after 30 days from the submission date.

3. A Secure Automated File Exchange (SAFE) account is required to submit completed templates and documentation. Refer to Section IV Step 3, below.

4. All new IaaS and PaaS cloud implementations must utilize CDT Security Operations

Center as a Service (SOCaaS) for continuous security monitoring and alerting. Additionally, all pre-existing IaaS and PaaS cloud implementations must utilize CDT SOCaaS for continuous security monitoring and alerting by June 30, 2025. Contact the Office of Information Security at security@state.ca.gov to initiate a SOCaaS exemption request.

5. Visit the California Cloud Services Assessment website for additional information.

III. California Cloud Services Assessment (CCSA) Documents Overview

A. General Assessment Questions

1. California Cloud Services Assessment Questionnaire

   This template contains questions pertaining to Agency/state entities cloud design.

2. Cloud Alternative Analysis

   This template contains questions for three Alternative Analysis along with the Total Cost of Owner (TCO) to assist Agency/state entities estimate costs specific to Cloud Computing. At least one alternative must include services available by CDT. Agency/state entities with existing Project Approval Lifecycle (PAL) Stage 2 Alternative Analysis can copy contents into the Cloud Alternative Analysis.

3. California Cloud Service Assessment Service Request

   The service request input screen will ask questions pertaining to a high-level description, business justification, business objectives, information pertaining to any related funding requests (i.e., Budget Change Proposals (BCP)), and California Department of Technology Projects in the PAL, or delegated projects.

   All documentation listed on the CCSA website "**Required Documentation Tab**" must be uploaded to the Secure Automated File Exchange (SAFE) account (See Section IV Step 3 for details).

B. Architecture Documents

1. Cloud Architecture & Network Diagrams

   The Cloud Architecture Diagram visually documents the organization's cloud computing services.

   See EXAMPLE A – CLOUD ARCHITECTURE DIAGRAM

   The Network Diagram visually documents the network flow for the cloud system and security inspection points.

   See EXAMPLE B – NETWORK DIAGRAM

2. Well-Architected Framework Assessment or equivalent from Cloud Service Provider (if a cloud account(s) exists)

The Well-Architected Framework Assessment or equivalent has been developed to help cloud architects build the most secure, high-performing, resilient, and efficient infrastructure possible for their applications. For more information on generating a report, please see your cloud service provider.

C. Security Documents

Information pertaining to existing security monitoring and operations must be provided. All new cloud implementations must use Security Operations as a Service or have an exemption. Please reference the Department of Technology services website for instructions on how to enroll or contact security@state.ca.gov.

To validate security requirements are met additional security information will need to be provided. Please complete the necessary templates for the assessment review.

Below is a list of the required security documentation:

1. Cloud System Security Plan (CSSP)

All cloud implementations are required to have a System Security Plan (SSP) for each system. If an SSP is not in place, a CSSP may be used. The CSSP is a lightweight SSP that enables State entities to initiate their cloud journey(s) with confidence. The CSSP serves as the solution blueprint and allows CDT to perform a high-level assessment for quality assurance prior to launch. The CSSP is not intended to substitute existing IT Security compliance requirements.

2. Privacy threshold and impact analysis State Information Management Manual (SIMM) 5310-C.
3. Classification Categorization Form – System Classification in the Federal Information Processing Standard (FIPS) 199.

Below is a list of security policies that will be reviewed against the documentation provided for the assessment:

- A current Technology Recovery Plan (TRP) with current systems submitted to CDT including, Business Impact Assessment (BIA), Recovery Time Objectives (RTO), and a Recovery Point Objectives (RPO).
- Alignment to Cloud Security Standard (SIMM 5315-B).
- Alignment with Cloud Security Guide (SIMM 140).
- Alignment with Cal-Secure goals & technical capabilities.
- Alignment with the National Institute of Standards and Technology (NIST) 800-207 Zero Trust Architecture.
- Alignment with Security Risk Assessment requirements the State Administration Manual (SAM) 5305.7.
- Alignment with Security Data Classification Assessment requirements (SAM 5305.5).
- Alignment with Security Privacy Impact Analysis requirements (SAM 5310.8).

D. Workforce Documents

To validate the necessary workforce planning requirements, the below documentation must be provided delineating which positions will support the cloud infrastructure.

Below is a list of the required workforce documentation:

- Organizational Chart of Cloud-related staffing

IV. Steps To Submit California Cloud Services Assessment (CCSA)

Below are the process steps to complete the service request for the cloud assessment.

Step 1 – Review the California Cloud Services Assessment (CCSA) Website Content
Perform the following tasks on the CCSA Website.

- Review the initial paragraphs on the background on the CCSA.
- Review "**Security Benefits Tab**"
- Review "**Roles & Responsibilities Tab**"
- Review "**Required Documentation Tab**"
- Review "**FAQs Tab**"
- Review "**SLO Tab**"

Step 2 – Review & Complete Templates and Prepare Documentation

- Download all the templates "**Required Documentation Tab**" by clicking on the links.
- Complete all required templates.
- Prepare additional required documentation.

Step 3 – Acquire a Secure Automated File Exchange (SAFE) account
This step can be done in parallel to the step above.

- Check with your Department ISO for an existing SAFE account.
- If there is no existing SAFE account, contact the Office of Information Security at security@state.ca.gov to create one. It will take approximately 1-2 days to complete.

Step 4 – Submit Request for California Cloud Services Assessment

NOTE: CDT IT Service Portal request system has a 15-minute timeout.

- Submit a Case/Request for "Off-Premises Cloud Services" in the CDT IT Service Portal.
- Answer ALL the questions in the service request.
- Notate Case/Request number (CSxxxxxx).

Step 5 – Submit Required Documentation

- Using the Case/Request number from the above step, create a folder with the following naming standard **[DeptAcronym]_CS[xxxxxx]_[file count]_CloudSmartMMDDYYYY** on a local machine.

  Example: CDT_CS001234_8_CloudSmart08112023

- Copy all the below documentation into the **[DeptAcronym]_CS[xxxxxx]_[file count]_CloudSmartMMDDYYYY** folder:

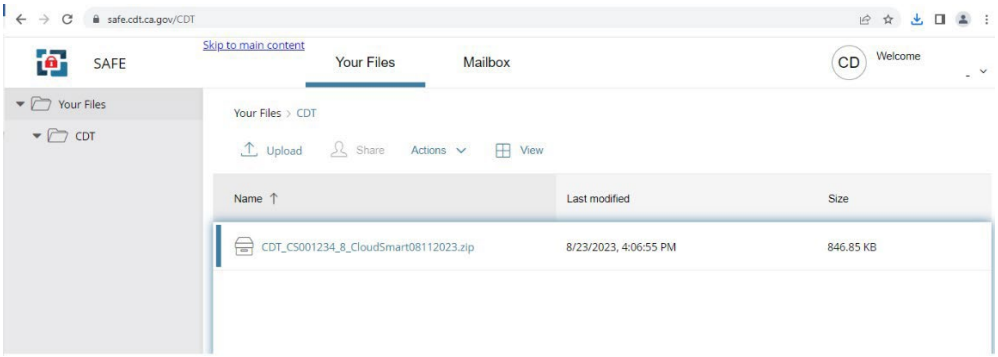
  1. California Cloud Services Assessment Questionnaire
  2. Classification Categorization Form – System Classification (FIPS 199)
  3. Cloud Alternative Analysis
  4. Cloud Architecture & Network Diagram (See Examples A & B)
  5. Cloud System Security Plan (CSSP)

6. Organizational Chart of Cloud-related staffing
7. Privacy Threshold and impact analysis (SIMM 5310-C)
8. Well-Architected Framework Assessment or equivalent from Cloud Provider (if you already have a cloud account)

- Zip the folder into a file

  Example: CDT_CS001234_8_CloudSmart08112023.zip

- Login to SAFE, then upload the Zip file using https://safe.cdt.ca.gov/



V. Questions

Questions regarding this guide may be sent to:

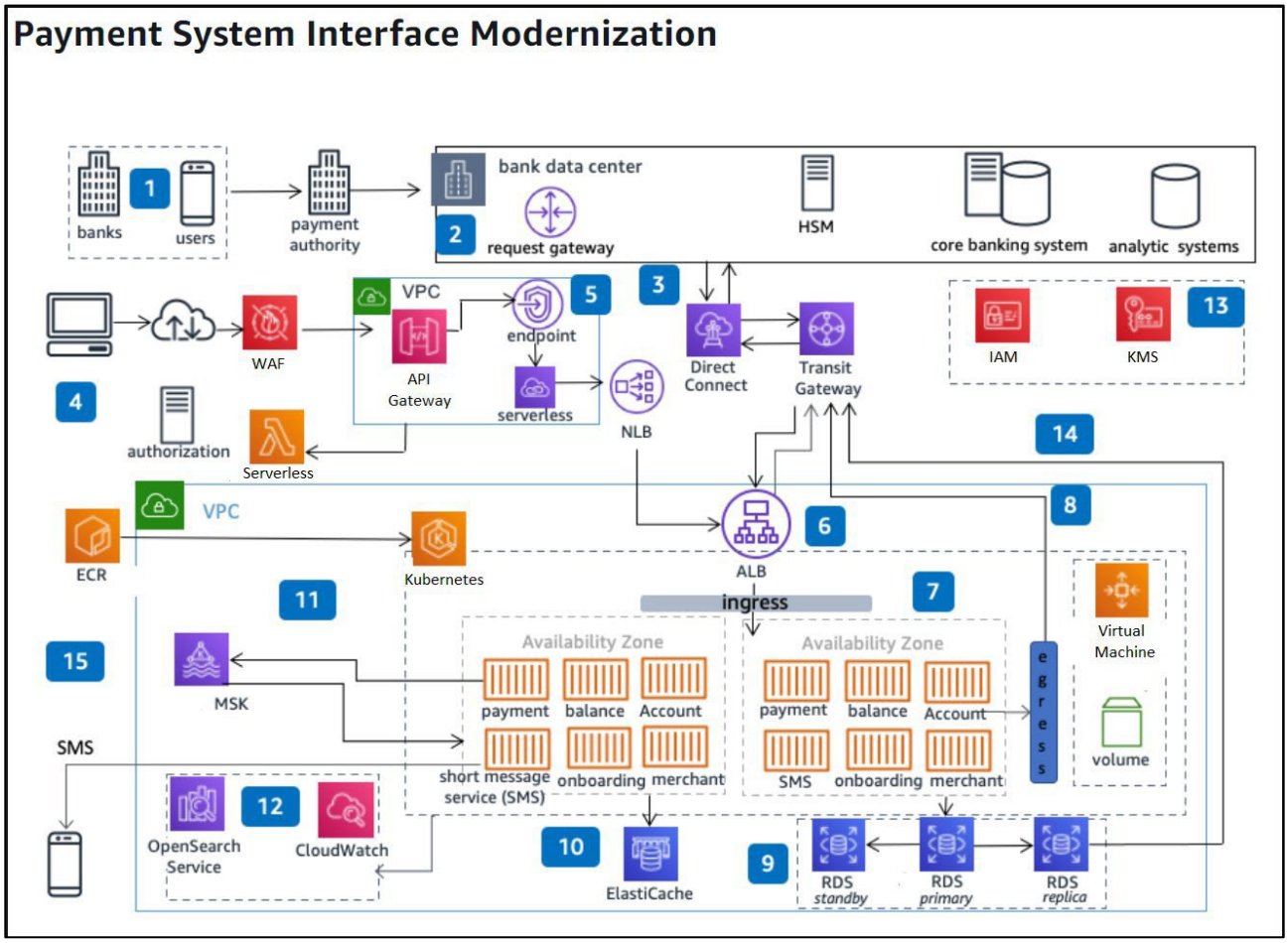
California Department of Technology

Office of Technology Services

Californiacloudservices@state.ca.gov

Example A – Cloud Architecture Diagram: Vendor Agnostic

The below diagram provides an example illustrating the level of detail required for the Cloud Architecture Diagram to be submitted for the CCSA process.



Example B – Network Diagram: Vendor Agnostic