California
DEPARTMENT OF TECHNOLOGY

Frequently Asked Questions
California Cloud Smart

CCSA Process and Requirements

1. Why is CDT implementing this new assessment process?

   - CDT is statutorily tasked with protecting the state's technology investment and mitigating risks. Cloud chaos limited our visibility into the environments for the state's critical data and services. Gathering data as customers come through the assessment will help us understand the technology portfolio in the cloud and ensure that standards, protocols, and security measures are being taken and also identify potential blind spots in our cybersecurity posturing.
   - Workforce is another driver, as we have seen customers migrate to the cloud but are not prepared to support that and have to have vendors operate on their behalf, inconsistent with GC19130.
   - We are resetting Cloud First expectation of migrating workloads, and establishing an integration strategy to ensure cloud is the best solution for certain workloads. If you are planning to modernize or moving a current system, your environment is going to change and there are benefits, features, and functionalities that CDT can help you select, as well as find the proper cloud that fits your requirements. By consulting with CDT to understand the business drivers of migrations, we can explore different scenarios for your environment so you can take advantage of the great features the cloud offers

2. Is the intent to achieve compliance with these policies for new and expanding cloud services only or for current services as well?

   The California Cloud Services Assessment (CCSA) is applicable to all cloud services but to allow for the most effective and reasonable implementation, the focus on different types of services will occur in phases. Phase 1 will focus on new cloud services requests. Engagement with customers around existing services will be included in Phase 2, beginning around Spring of 2024.

   a. For existing cloud customers, what is considered a modification to an existing system? What conditions can trigger an assessment?

      A CCSA will be required for customers requesting a new system/environment, a new service under an existing system/environment, or a change from one service to another. Any type of major architectural changes, changes to data classifications, expanding services where it will have a significant impact on other ancillary, feeder, or downstream systems, or if it is public facing will all trigger the CCSA review. Examples of systems/environments include, but are not limited to, AWS Accounts, Azure Account Owner/Subscriptions, Google Project, Oracle (OCI) Tenant, etc.

      If there are no changes to previously submitted documentation, workforce, or architecture, then the CCSA process may not be required. For additional guidance, please contact your Account Lead.

   b. Does the CCSA apply to cloud accounts or individual solutions hosted in the cloud accounts?

      The CCSA applies to each system or solution that is hosted in your cloud account.

   c. Do departments have to follow the CCSA process for account inquiries or modifications?

      Customers requesting information about existing cloud services or requesting modifications to account users should utilize the **Off-Premises Cloud User Maintenance** catalog item.

3. How do I initiate the CCSA? Is there a form?

Review the California Cloud Services Assessment webpage for requirements and instructions. Initiation of the CCSA has been integrated within the existing Off-Premises Cloud Services Request catalog item in CDT's IT Service Portal.

4. Is the 14-[business] day review time an SLA from CDT? Will the 14-[business] days start over for each review cycle?

   It is a Service Level Objective, contingent upon complete documentation and timely response from customers to any questions.

   CDT does not anticipate follow-up reviews. Each review will be for a new account or change to cloud. The 14-business days will restart if there is incomplete or missing documentation in the request.

   CDT has adequate resources to ensure we meet this SLA and the CCSA is not a bottleneck for requests. Additionally, if there is a rational need or urgency, we will work with customers to prioritize those requests accordingly.

5. What is the cost for the CCSA process?

   There is currently no cost associated with the CCSA process. Any future costs will be published in CDT's service rates catalog.

6. How does this process align with the CDT Project Approval Lifecycle (PAL) Process?

   Customers will initiate the CCSA either during stage 2 or state 3, depending on the type of procurement. Once a solution is identified and the architectural planning is underway, the customer should initiate the CCSA process. The CCSA review team will coordinate with CA-PMO.

   a. Does the CCSA apply to initiatives that fall below the threshold for CDT oversight or PAL?

      All IaaS and PaaS off-prem cloud service requests will be required to follow the CCSA. CDT's CAMC services are not subject to the CCSA.

7. What additional or modified audits will be conducted? Will they be security or architectural related? What is the frequency?

   In addition to existing security audits, periodic configuration, service health checks, and compliance inspections will be conducted. Health checks evaluate the operational efficiency, robustness, and security of a cloud system and can also help identify potential risks of current cloud architecture.

8. Does the CCSA apply to FedRAMP compliant cloud providers?

   Yes. A CCSA is required for all Off-Prem requests. The CCSA is not required for requests for CDT Managed Cloud (CAMC) services.

9. Where can I find a list of CDT's approved cloud services?

   CTD approved cloud services: https://cdt.ca.gov/services/cloud-services/

10. What On-Prem Cloud Solutions are included in CAMC?

    For CAMC details, visit: California Managed Cloud Hosting

11. What is my Account Code (required to submit CCSA request)?

    Each Department is assigned one (or more) account billing codes. If you do not know your department's Account Code, contact your CES account representative.

12. Will training be offered on the request process in a portal format such as CalLearns?

At this time, detailed instructions on the CCSA request process can be found in SIMM 141 California Cloud Services Assessment Guide. Additional training and guidance will be available to state employees via forums and regular communication from CDT.

Customers can review knowledge articles specific to the request processes: CDT IT Service Portal

13. What cloud elements will require SOCaaS monitoring?

    SOCaaS is mandatory for all state departments. Per SIMM 141, all pre-existing IaaS and PaaS cloud implementations but be subscribed by June 30, 2025. Please review the CDT Security Operations Center webpage for service details.

    Security Operations Center as a Service (SOCaaS) - CDT Services

14. What are the costs for SOCaaS?

    SOCaaS monitoring and alerting is free to state entities, however, there are opportunities to incur costs. If a customer has additional requirements (e.g., retention policy) to keep logs, they are responsible for the costs of storing the data. Customers will not pay for monitoring and alerting of logs.

15. Is there an exemption to SOCaaS?

    Agencies/state entities with existing monitoring services can work with CDT's Office of Information Security on a case-by-case basis, to determine monitoring needs, requirements, and exemptions. Contact your Account Lead to initiate this process.

16. Are updated architecture diagrams required when changes are made? If so, what is the timeframe for which they will need to be submitted?

    Engagement with customers around existing services will be included in Phase 2, beginning around Spring of 2024. Please contact your CES account lead if you need CDT assistance in preparing a diagram to be ready for the effective date.

17. Is the Cloud System Security Plan (CSSP) required for all current operational systems, or just for the new requests?

    The System Security Plan (SSP) is in addition to the requirements outlined in SAM. Customers are already required to complete an SSP for each system that is in operation. When you initiate a cloud request, we are asking you to present that SSP with just the pertinent information for evaluating cloud requests, in the form of the CSSP. Customers are still required to comply with SAM and complete all required documentation.

18. Do the TRPs need to be updated with release of the new policies?

    This is already an existing requirement and has not changed. TRPs will be validated during the California Cloud Assessment. If state entity is not planning to submit a CCSA request for new services, they should ensure the TRP is updated per existing SAM requirements.

    a. Technology Recovery Plans (TRP) are updated annually, so new initiatives may not be captured.

       TRPs are an existing requirement and should address current systems, not planned systems. As per the current process, TRPs should be updated to include new systems, once implemented.

19. Can services be procured through Cloud Service Provider Marketplaces?

    Departments must ensure compliance with the State Contracting Manual when procuring additional products and services available in cloud online Marketplaces. When possible, additional products and services should be procured through department procurement offices to ensure purchasing regulations and requirements are met. Negotiated contract pricing is not applicable to Marketplace products and services and IaaS or PaaS services are recommended to be procured through CDT's negotiated contracts.

20. Are exemptions allowed for special circumstances?

    There are no exemptions to the CCSA review process. If CDT's Cloud service offerings do not satisfy requirements, a Cloud Exemption Request (SIMM 18B) may be submitted, following existing processes. As we progress, CDT will be considering a delegated authority type of approach, whereas when a department demonstrates they are successfully meeting the policies and requirements to migrate workloads into the cloud, CDT may no longer need to have the documents submitted to us. From there, it will be periodic assessments, similar to the California Department of Military audits, to ensure the solutions and systems are maintained over time.

Cloud-Based Services

1. Is a CCSA required for cloud service variants (e.g., aPaaS and iPaaS)?

   Contact your Account Lead to initiate discussions and prior to submitting through the CCSA process. CDT SMEs can help determine requirements for aPaaS and iPaaS on a case-by-case basis.

2. Does the CCSA apply to StaaS requests?

   If utilizing CDT's On-Prem STaaS, requests would not go through assessment. If using CDT's off-prem cloud contract, CCSA applies.

3. Are SaaS requests required to go through the CCSA?

   Currently, only requests for Off-Prem IaaS and PaaS solutions require the CCSA. CDT will begin integrating SaaS services in the CCSA process towards the end of 2024.

4. Is an exemption from CDT required to utilize other commercially available SaaS solutions (DGS)?
   An exemption from CDT is not required.

5. What SaaS Solutions must be procured through CDT?

   Visit CDT's SaaS catalog for a listing of solutions. At this time, all other SaaS products should be procured through the DGS procurement mechanisms.