State of California

Department of Technology

Stage 2 Alternatives Analysis

Version 3.0.3

Preparation Instructions

Statewide Information Management Manual – Section 19B

February 2022

INTRODUCTION TO
THE STAGE 2 ALTERNATIVES ANALYSIS

Overview

Statewide Information Management Manual (SIMM) Section 19B, Stage 2 Alternatives Analysis (S2AA), is the second stage of the Project Approval Lifecycle (PAL) and provides a basis for project management, program management, executive management, and state-level control agencies to understand and agree on how the proposal's business objectives will be achieved, to evaluate multiple alternative solutions, determine which alternative will yield the highest probability of success, and to develop an acquisition strategy/plan for procuring services if needed. The Stage 2 Alternatives Analysis instructions have been prepared to help State of California agencies and state entities[1] meet the California Department of Technology (CDT) requirements for documentation of proposals for projects.

Clarifications

- ✓ A Stage 1 Business Analysis must be approved by the CDT (or Agency Information Officer for agency-affiliated state entities and acknowledged by CDT) prior to conducting a Stage 2 Alternatives Analysis.
- ✓ Proposal reporting requirements are initially determined as part of the Stage 1 Project Reportability Assessment but may change as the proposal progresses though the PAL.
- ✓ For proposals anticipated to be non-delegated, agencies/state entities are required to submit a Stage 2 Alternatives Analysis to the CDT.
- ✓ For proposals anticipated to be non-delegated, a Stage 2 Alternatives Analysis must be approved by the CDT prior to submitting a Stage 3 Solution Analysis.
- ✓ For proposals anticipated to be delegated, agencies/state entities must receive Stage 2 Alternatives Analysis approval from the agency/state entity's Director, as applicable.

Stage 2 Alternatives Analysis Reporting Requirements

For proposals that are anticipated to be non-delegated, the CDT requires specific information from agencies/state entities to carry out its responsibilities in approving the Stage 2 Alternatives Analysis. To evaluate an agency/state entity's Stage 2 Alternatives Analysis, the CDT needs to fully understand the business investment justification. Each proposal must provide sufficient detail to describe the baseline processes, business requirements/outcomes, viable alternative solutions, and staffing plan.

Each agency or state entity is responsible to ensure its Stage 2 Alternatives Analyses meet CDT requirements. The Stage 2 Alternatives Analysis must be comprehensive and cannot rely on verbal or subsequent written responses (e.g., emails) to the CDT staff's questions to provide needed justification for the submission. Incomplete submissions that fail to provide relevant information in written form may be returned without consideration at the discretion of the CDT.

The CDT may, at its discretion, request additional information from the agency or state entity.

[1]**State entity:** Includes every state office, officer, department, division, bureau, board, and commission, including Constitutional Officers. "State entity" does not include the University of California, California State University, the State Compensation Insurance Fund, the Legislature, or the Legislative Data Center in the Legislative Counsel Bureau.

Changes to Previously Approved Submittals

As a proposal progresses through each stage of the PAL, further analysis is conducted, uncertainties are cleared, and data used for decision-making improves. As additional information is collected (e.g., cost estimates, schedules, and business objectives), the information submitted in an earlier stage can be refined. If information from a previously approved Stage 1 Business Analysis needs to be updated, the agency/state entity should submit an updated Stage 1 Business Analysis along with the Stage 2 Alternatives Analysis submittal.

Changes to Reportability Status

If at any stage in the PAL a proposal initially anticipated to be delegated now meets any of the reportability criteria as per State Administrative Manual (SAM) 4819.37, the agency/state entity is required to resubmit a Stage 1 Business Analysis, Stage 1 Project Reportability Assessment, and Stage 2 Alternatives Analysis with all sections completed for CDT review and approval.

Microsoft (MS) Word Version Forms

To ensure California's compliance with the Americans with Disabilities Act (ADA) as Amended, the CDT will only support and accept for submission the Stage 2 Alternatives Analysis version 3.0 (MS Word form) starting February 28, 2022. The submissions will be checked for ADA compliance and returned to the department if ADA guidelines are not met.

Stage 2 Alternatives Analysis Version 3.0 Changes

The Stage 2 Alternatives Analysis version 3.0 contains the following changes:

- The form no longer uses tables as a means of organizing content.
- Sections that required check boxes are now drop-down fields or narrative areas.
- The iterative sections will now be cut and pasted by the user manually.
- Sections that require artifacts to be attached to the word document will now be required to be submitted as attachments to the submission email.
- Sections originally 2.2 Preliminary Submittal and 2.3 Stage 2 Preliminary Assessment removed. Content moved to Stage 1 Business Analysis or Project Reportability Assessment as needed.
- Many documents are being asked to be submitted with this proposal. CDT can accept up to 25MB of attachments per email, 1000 document count limit.
- Sections that previously required inputting data from attachments have been pared down to allow for minimal information along with submission of the attachments instead.

Stage 2 Alternatives Analysis Transmittal Requirements

The Project Approval Executive Transmittal Form, located in SIMM Section 19G, will be used to satisfy the transmittal requirements for Stage 2 Alternatives Analysis.

- ✓ State entities are required to sign and submit the Project Approval Executive Transmittal to their governing agency for approval.
- ✓ Agencies are required to sign and submit the Project Approval Executive Transmittal to the CDT.

Please note that wet signatures and electronic signatures are accepted.

Exception – State entities that are not governed by agencies can sign and submit the Project Approval Executive Transmittal directly to the CDT.

Project Approval Executive Transmittal

The Transmittal template (available in SIMM Section 19G) contains the approving agency/state entity executive signatures, with the following components:

1. **State Entity Name:** Enter the state entity name that prepared the Stage 2 Alternatives Analysis. Designate one state entity as owner if multiple state entities have a role in the proposal.
2. **Agency Name**: Enter the agency name that prepared the Stage 2 Alternatives Analysis. Designate one agency as owner if multiple agencies have a role in the proposal. This field is not required for state entities not governed by an agency.
3. **Organization Code**: Select the organization code for the state entity responsible for the proposal.
4. **Name of Proposal:** Enter the proposal name as determined by the agency/state entity in the approved Stage 1 Business Analysis.
5. **Department of Technology Project Number**: Enter the project number assigned by the CDT during the Stage 1 Business Analysis (in “0000-000” format).
6. **Submission Deliverable**: Select the Stage/Gate deliverable(s), as applicable.
7. **Approval Signatures:** The agency/state entity executive approval signatures are required, documenting commitment and involvement at the agency/state entity level. The required signatures include those of the Information Security Officer, Enterprise Architect, Chief Information Officer, Budget Officer, State Entity Director, Agency Information Officer and the Agency Secretary.

Table of Contents

Stage 2 Alternatives Analysis Main Form Instructions

2.1 General Information

Agency or State Entity Name: Select the agency/state entity name that prepared and is responsible for the Stage 2 Alternatives Analysis proposal. Designate one agency or state entity as owner if multiple agencies or state entities have a role in the proposal. Includes the Organization Code in the dropdown list.

> **If Agency/State entity not in list, enter here:** Enter the agency/state entity if not in dropdown list above including Organization Code.

Proposal Name: Enter the proposal name and acronym as determined by the agency/state entity.

Department of Technology Project Number: Enter the number assigned by the CDT in Stage 1 (in "0000-000" format).

S2AA Version Number: Select the version of the current S2AA. This selection should be used to keep track of the active document.

CDT Billing Case Number: Enter the Case Number issued by CDT's ServiceNow system for billing. If you do not have a Case Number, please click on the link in the S2AA form to access the ServiceNow page. A request can be placed through this service to obtain a case number for billing.

2.2 Submittal Information

Contact Name: Enter the name for agency/state entity person who will be the primary point-of-contact for control agency questions and comments.

Contact Email: Enter the email address of the contact provided above.

Contact Phone: Enter the ten-digit phone number of the contact provided above.

Submission Type: Select one of the following types of submission.

> **New Submission**: Initial submission to the CDT.
>
> **Updated Submission (Pre-Approval):** Updated submission based on review and feedback from the CDT, critical partners or other stakeholders prior to formal approval.
>
> **Updated Submission (Post-Approval):** If Stage 2 Alternatives Analysis has been previously approved by the CDT and new information or updates are required, the submittal should be updated based on new information. For instance, as a proposal progresses through each stage of the PAL, further analysis is conducted, uncertainties are cleared, and data used for decision-making improves, in this case an update to the Stage 2 Alternatives Analysis may be required.
>
> **Withdraw Submission:** An agency/state entity may decide to withdraw the Stage 2 Alternatives Analysis for various reasons (e.g., change in direction, feasibility, budgetary issues). If an agency/state entity wishes to withdraw a previously submitted or approved proposal from further consideration, check this field and submit the Stage 2 Alternatives Analysis to the CDT.

If “Withdraw Submission” is selected, select the reason for the withdrawal from the dropdown menu. If “Other,” specify the reason in the space provided.

Contact your CDT Office of Statewide Project Delivery (OSPD) Project Approval and Oversight Manager and Agency Information Officer (if applicable) to inform them of your intention to withdraw the proposal. The CDT will send a written confirmation of withdrawal and communicate to all associated stakeholders. Once a proposal is withdrawn, the agency/state entity will be required to submit a new Stage 2 Alternatives Analysis to continue with a proposal for the same or a similar request.

Sections Changed, if an update or a resubmission: If either Submission Type “Updated Submission (Pre-Approval)” or “Updated Submission (Post Approval)” is selected, then enter the section numbers where updates have been made.

Summary of Changes: Provide a concise summary of changes made.

TIP: Highlight or otherwise indicate new or changed text within the modified section.

Project Approval Executive Transmittal: Include a copy of the signed Project Approval Executive Transmittal for Stage 2 Alternatives Analyses with your submission; use the Transmittal Form located in SIMM Section 19G.

Procurement Assessment Form: Include a copy of the B.5 STP Procurement Assessment form with your submission. This form needs to be filled out with all information required for Stage 2. The STP Procurement Assessment Form can be found in SIMM Section 19B.

Conditions from Stage 1 Approval: Add any conditions from the Stage 1 Approval placed on the project by CDT (for non-affiliated departments) or by your AIO (for agency-affiliated departments).

2.3 Baseline Processes and Systems

An understanding of current business processes (which may include manual processes) and supporting systems, also known as the current “as is” solution (if any), is needed to successfully perform an effective alternatives analysis.

2.3.1 Current Business Environment

Provide a brief narrative description of the current baseline business processes with their associated costs that will be impacted by this proposal. Attach current Business Environment diagrams for all existing business processes related to this proposal to your email submission. The Current Business Environment consists of mapping a series of necessary business functions that depict an abstract graphical view of real work and personnel under different situations or timeframes. The workflow should include the events that initiate each process (i.e., the trigger event) and the results of those processes. The attachments must be in Portable Document Format (PDF) or Microsoft Visio format. The costs for the current business environment will be required to be submitted in the Financial Analysis Worksheet, covered in Section 2.12. The workflow should include the following components:

- Business Process – Illustrate the active roles and the activity the role conducts during the business process. Include the parallel processes as well as sequential steps in a process that execute the successful completion of the business process.
- Business Rules – Any business policies or procedures that dictate the need for the business process.

- Trigger Events – One or more events that directly start a business process (e.g., receive a request, phone call, or a scheduled date).
- Results – One or more outcomes from the execution of a business process.
- Data Dictionary – List of database files, number of files, relationships to other data, and elements that depict the data structure. This documentation may be submitted along with the workflow diagram.

2.3.2 Technical Context

Provide a brief narrative description of the current baseline systems that will be impacted by this proposal. The agency/state entity business and technical teams will collaborate to complete the information. The business team will complete, or provide to the technical team, the business processes for the current solution. The technical team will complete, or provide to the business team, the technical-related items (e.g., application, system, or component; Commercial off-the-shelf (COTS), Cloud-based, or custom solution; runtime environment; system interfaces; data center location; and, security).

Document each business process and the supporting technology for the current solution. Only discuss business programs and supporting technology affected by the proposal as identified in the Stage 1 Business Analysis. If a business process is completely manual and does not currently have any supporting technology, only identify the business process. The Technical Context should align with Section 2.3.1 Business Context. For each business process identified, provide the following in attachments:

Application, System, or Component: Enter the name of the application, system or component that supports the associated business process.

COTS/Cloud Technology or Custom: Select either “Commercial off-the-shelf (COTS)/Cloud,” “Modified off-the-shelf (MOTS)” or “Custom solution” to identify the type of application, system or component used. For a COTS/Cloud or MOTS product, provide the name of the COTS/Cloud or MOTS product utilized in the system.

- COTS/Cloud product – Typically, a ready-made computer hardware or software product for specific uses and available for sale to the general public. COTS/Cloud products are designed to be installed without requiring custom development. For example, Microsoft Office is a COTS product that is a packaged software solution for businesses and individuals. Microsoft SharePoint Online is an example of a Cloud solution for businesses. The Federal Acquisition Regulation (FAR) defines the rules for COTS products.

- MOTS product – Typically, a COTS product with source code made available to the purchaser to allow for modifications. The product may be customized by the purchaser, by a vendor, or by another party to meet the requirements of the customer. Since MOTS product specifications are written by external sources, purchasers may not have control of future changes to the product.

- Custom solution – Typically, computer software developed for a specific customer to accommodate the customer's particular requirements, preferences, and expectations.

Name/Primary Technology: For a custom solution, enter the primary technology used to build the system (e.g., .NET, Java).

System Interfaces: Enter the name(s) of system(s) that exchange data with the current system using interface files, web services, etc. Identify systems within scope of the proposed project that interface with each other. Also identify systems outside the scope of the proposed project that interface with the baseline systems. Provide a brief description of the purpose of each interface. If the system exchanges data with other entities, specify the name of the entity. Examples include but are not limited to the following:

- Federal partners
- Local city/county partners
- State agency entity partners
- Judicial branch
- Universities
- Researchers

Data Center Location: Select the location of the data center where the current system is hosted.

- State Data Center: A data center operated by the CDT, Office of Technology Services (OTech).
- Agency/State Entity Data Center: A data center independently operated by an agency/state entity.
- Commercial Data Center: A data center operated by a solution provider or vendor contracted by the agency/state entity.
- Other: If not one of the above, type the location of the data center where the current system is hosted.

Security: Section used to indicate the security and privacy characteristics of the current system.

Access: Select Yes or No for each access type to identify who is authorized to access the current system:

- Public: Select Yes if the current system is accessible to public parties with or without restricted access.
- Internal State staff: Select Yes if the current system is accessible to internal state staff with or without restricted access.
- External State staff: Select Yes if the system is accessible to state staff from other agencies/state entities, with or without restricted access.
- Other. Specify who else is authorized to access the current system.

Type of Information: Select Yes or No for each to identify the type of information that requires protection. See the SAM Section 5305.5 for more information.

- Personal: Select Yes if personally identifiable information (e.g., social security numbers, demographic information) is collected, processed and/or presented by the system.
- Health: Select Yes if diagnosis, treatment, provider, insurance, or billing information is collected, processed and/or presented by the system.
- Tax: Select Yes if IRS safeguards or state or local tax information policies (similar to the Federal IRS safeguards) are required to protect information contained in state or local tax submissions.
- Financial: Select Yes if confidential or sensitive financial information is maintained (e.g., payment processing, salaries, budget, credit card numbers, contract amounts).

- Legal: Select Yes if confidential or sensitive legal information is maintained (e.g., arrest records, court records, incarceration records, contracts, lawsuits, legal documents).
- Confidential: Select Yes if other types of confidential or sensitive information are maintained by the system (e.g., business trade secrets, investigations, enforcement actions).
- Other. Specify the type of information that requires protection.

Protective Measures: Select Yes or No to identify the protective measures used to protect information.

- Technical Security: Select Yes if hardware and software security measures (e.g., firewalls, virus protection, intrusion detection/prevention) are used to protect the networks, servers, workstations, and other devices in the infrastructure.
- Identity Authorization and Authentication: Select Yes if the current system requires restricted access to either state employees and/or to the public.
- Physical Security: Select Yes if servers and network devices are secured with environmental security measures (e.g., door locks, surveillance equipment).
- Backup and Recovery (Technology Recovery): Select Yes if data is backed up and stored offsite.
- Other, specify: If other, specify how the information is currently protected.

TIP: A similar set of information will be asked for in Section 2.8, copy/paste from Section 2.8 as needed.

2.3.3 Data Management

Enter the information to indicate the data owner and data custodian of the current system.

Data Owner (Owner of information assets): Identify the individual and the organizational unit with the responsibility for making classification, categorization, and control decisions regarding information assets. See SAM Section 5305.5 for more information.

- Data Owner Name: Enter the name of the Data Owner.
- Data Owner Title: Enter the title of the Data Owner.
- Data Owner Business Program: Enter the name of the Business Program with controlling ownership of the data.

Data Custodian (Custodian of information): Identify the individual and their organizational unit which is the caretaker for the proper use and protection of information assets on behalf of the information asset owner (e.g., a data center or information processing facility). See SAM Section 5305.5 for more information.

- Data Custodian Name: Enter the name of the Data Custodian.
- Data Custodian Title: Enter the Title of the Data Custodian.
- Data Custodian Business Program: Enter the name of the Business Program that is the custodian of the data.

2.3.4 Existing Data Governance and Data

Data is a critical business asset and the foundation of valuable intellectual property. Unless valid, complete, accurate, and compatible data components are available, the maximum value of the

proposed solution cannot be obtained. Therefore, it is crucial that an agency/state entity evaluate its readiness to undertake the initiative with a full understanding of the preparation and resources required.

Data governance refers to the implementation of data management processes, policies, procedures, standards on how critical business data decisions are identified and made, and the availability, usability, integrity, and security of data.

A data governance program should include a governing body (e.g., a steering committee or council) with well-defined roles and responsibilities, and established processes and procedures to carry out the governance program. The data governance body or program is responsible for:

- Defining business data owners and data custodians for data assets
- Developing policies that specify who is accountable for the data and its accuracy, accessibility, consistency, completeness, and timeliness
- Defining processes on how the data is to be stored, archived, backed up, and protected from mishaps, theft, or attack
- Developing standards and procedures to define how the data is to be used by authorized personnel
- Implementing a set of controls and audit procedures to ensure ongoing compliance with applicable laws, rules, and regulations
- Data governance related artifacts may include:
    - Data governance organizational chart
    - Data roles/responsibilities
    - Data policies, standards, procedures
    - Data strategy

Select an option for each of the following questions:

Do you have existing data that must be migrated to your new solution?

Select "Yes" if the proposal will require data conversion/migration activities.

If "Yes," include your data migration plan, draft or complete, as an attachment to your email submission. If your data migration plan has not been started, please indicate the status and expected completion date.

If data migration activities are required, use the dropdown to rate the data quality.

Does the Agency/state entity have an established data governance body with well-defined roles and responsibilities to support data governance activities?

Does the Agency/state entity have data governance policies (data policies, data standards, etc.) formally defined, documented, and implemented?

Data governance refers to the implementation of data management processes, policies, procedures, standards on how critical business data decisions are identified and made, and the availability, usability, integrity, and security of data. The data governance policies and process may include:

- Defining business data owners and data custodians for data assets

- Defining processes on how the data is to be stored, archived, backed up, and protected from mishaps, theft, or attack
- Developing standards and procedures to define how the data is to be used by authorized personnel
- Implementing a set of controls and audit procedures to ensure ongoing compliance with applicable laws, rules, and regulations

Select "Yes" if the agency/state entity has data governance artifacts and provide attachment with your email submission.

Does the Agency/state entity have data security policies, standards, controls, and procedures formally defined, documented, and implemented?

Data security management refers to the implementation of security policies and procedures that provide for the proper authentication, authorization, access, and auditing of data and information.

The data security program objective is to:

- Properly manage and control access and changes to data assets
- Meet regulatory requirements for privacy and confidentiality
- Ensure that the privacy and confidentiality needs of all stakeholders are met

Data security management artifacts may include:

- Data security policies and standards
- Data security controls and procedures
- Data/information classifications
- Data security audits
- Data privacy and confidentiality standards
- User profiles, passwords and memberships

Select "Yes" if the agency/state entity has formally defined, documented, and implemented data security policies, standards, controls, and procedures.

Does the Agency/state entity have user accessibility policies, standards, controls, and procedures formally defined, documented, and implemented?

User accessibility policies, standard, and controls ensure that users are able to interact with systems and conduct business transactions regardless of disability status. User accessibility artifacts may include:

- Web accessibility standards
- Americans with Disabilities Act (ADA) compliance review bodies

Select "Yes" if the agency/state entity has formally defined, documented, and implemented accessibility policies, standards, controls, and procedures and provide as an attachment to your email submission.

2.3.5 Security Categorization Impact Table

Attachment: Attach a table (in PDF) that categorizes and classifies the agency/state entity's information assets (e.g., paper and electronic records, automated files, databases requiring appropriate protection from unauthorized use, access, disclosure, modification, loss, or deletion).

The categorization and classification of information assets is a prerequisite for determining the level of protection needed. Each information asset for which the agency/state entity has ownership responsibility shall be inventoried and identified. Refer to SIMM 5305-A Information Security Program Management Standard for additional information on security categorization. The Information Security Officer (ISO) will assist in the business and organizational security risk assessment of information assets. Use the following groups to categorize and classify the information assets:

- Public Information [not exempt from disclosure under Government Code (GC) Sections 6250-6265].
- Confidential Information (exempt from disclosure under GC Sections 6250-6265 or has disclosure restrictions in accordance with other applicable state or Federal laws)
- Sensitive Information (which requires special precautions to protect from unauthorized use, access, disclosure, modification, loss, or deletion).
- Personal Information (e.g., Social Security Number, driver's license/California identification card, financial account number, medical/health information).
- Description and useful value of the information asset.
- Owner of the information asset.
- Custodians of the information asset.
- Users of the information asset.
- Classification of information.
- FIPS Publication199 categorization and level of protection (Low, Moderate, or High).
- Importance of information asset to the execution of the state entity's mission and program function.
- Potential consequences and impacts if confidentiality, integrity and availability of the information asset were compromised.
- Potential consequences and impacts if confidentiality, integrity and availability of the information asset were compromised.

SIMM 5305-A Information Security Program Management Standard, Information Asset Owners, Responsibility, Number 3, provides:

> "Subject to executive management review, classifying information assets, including each record, file, or database for which it has ownership responsibility in accordance with the need for precautions in controlling access to and preserving the security and integrity of the information asset."

Refer to the Federal Information Processing Standards (FIPS) Publication 199 and SIMM 5305-A for additional information regarding the categorization and classification of information assets:

http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.)

SIMM 5305-A Information Security Program Management Standard).

2.3.6 Security Categorization Impact Summary

Select "Low," "Moderate," or "High" for each security objective category (i.e., Confidentiality, Integrity, and Availability) from FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*. The summary security categorizations are further detailed below:

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Low
The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.

Moderate
The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.

High
The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

***Integrity*:** Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

Low
The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.

Moderate
The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.

High
The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Availability: Ensuring timely and reliable access to and use of information.

Low
The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.

Moderate
The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.

High
The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

When determining the security objective categorization, consider the impact if the information does not remain confidential, the measures required to maintain authenticity and guard against unauthorized modification or removal, and the disruption caused if the information is not maintained or updated.

2.3.7 Technical Complexity

Use the SIMM Section 45 Appendix C, Complexity Assessment Template self-assessment tool to complete the **Technical Complexity** section based on the applicable information captured in the Stage 2 Alternative Analysis. Enter the Technical Complexity score in the space provided and attach the completed Appendix C (Business Complexity is used in the Stage 1 Business Analysis) to your email submission.

2.4 Requirements and Outcomes

Attachment: Email the requirements or outcomes detail in Excel, PDF or another electronic format.

A requirement is a documented representation of a condition or function that must be met or possessed by a solution or solution component to satisfy a contract, standard, specification, or other documented criteria. The main objective or goal in defining requirements is to communicate stakeholder objectives, needs, and outcomes. In the Stage 1 Business Analysis, business goals and objectives form the initial business requirements for the proposal. Business process workflows produced during Stage 2 Alternatives Analysis provide business context for further elaboration of the business requirements into requirements (i.e., functional, non-functional, and project/transition requirements) and outcomes (i.e. expected results or product) defined in Stage 2. Requirements and Outcomes specify the conditions, functionality, quality of service, and capabilities a solution must have in order to meet the business need or solve the business problem as described in the Stage 1 Business Analysis. For the purposes of the PAL, requirements and outcomes (or user stories) are sub-classified into functional requirements, non-functional requirements, and project/transition requirements. Requirements and Outcomes enable an agency/state entity to:

- Evaluate multiple alternative solutions
- Determine which alternative will yield the highest probability of success
- Develop an acquisition strategy/plan for procuring services if needed

The Stage 2 Alternatives Analysis Requirements and Outcomes serve as a bridge between business objectives established in Stage 1 and the more detailed solution requirements developed as part of the Stage 3 Solution Development, as summarized below:

Requirements in the Project Approval Lifecycle

Stage 1 – Business Analysis

- **Business Requirements** – Goals, objectives and outcomes identified.
- **Stakeholder Needs Captured.**

Stage 2 – Alternatives Analysis

- **Process Flows** – The graphic representation of the business processes.
- **Mid-Level Solution Requirements** – Characteristics of a solution scope and quality of service.
- **Functional Requirements** – Feature level information to validate the size of the system.

- **Non-Functional Requirements** - Information to validate alternatives.
- **Project/Transition Requirements** – Information to validate the feasibility of cost and schedule.

Stage 3 – Solution Development

- **Detailed Functional Requirements** – Information to ensure the system meets stakeholder needs.
- **Detailed Non-Functional Requirements** – Information to ensure the system operates as required; identifies qualities of the system and constraints on the system.
- **Detailed Project/Transition Requirements** – Information to ensure the system is built on time and budget and meets quality levels.
- **Detailed Mandatory/Optional Requirements** – Information on optional requirements (e.g., maintenance and operations after first year of operations) that will be implemented at the option of the state.
- **Administrative Requirements** – Requirements that are defined by the CDT, OSPD STP and included under a separate section of a solicitation.

Stage 4 –

Project Readiness and Approval

- **Finalized Functional Requirements** – Information to test and subsequently maintain the desired functionality in the system.
- **Finalized Non-Functional Requirements** – Information to test and subsequently maintain the quality and operational aspects of the system, within the defined constraints.
- **Finalized Project/Transition Requirements** – Information to test and subsequently maintain the quality, budget and time constraints.
- **Finalized Mandatory/Optional Requirements** – Information to subsequently maintain and validate the need to implement optional requirements (e.g., maintenance and operations after first year of operations).

Refer to SIMM Section 19B.3 for the Mid-Level Solution Requirements Template to document requirements. The Mid-Level Solution Requirement Template Instructions are provided below. The Mid-Level Solution Requirements Template introduces a component of traceability that is initially developed as part of Stage 2 Alternatives Analysis and will be further elaborated in Stage 3 Solution Development. Traceability will help to ensure that what is delivered by the completed solution is neither more nor less than what was agreed to by the project stakeholders. See SIMM 17 California Project Management Framework (CA-PMF) for a sample Traceability Matrix and user instructions.

Alternatively, agencies/state entities may choose to document their requirements and outcomes via “Epics/User Stories.” If “Epics/User Stories” are used, the agency/state entity will be required to provide detailed functional requirements in Stage 3 Solution Development. References have been provided:

Requirements References:

- SIMM 170 Requirements Guidelines
- Project Requirements Development Instructions
- Requirements Traceability Matrix

- Strong Requirements Example
- Requirements Gathering Workflow
- Business Analysis Body of Knowledge

Epics/User Stories References (if adaptive methodology is followed):

- Agile methodology guidelines
- GSA User Story Guidelines
- User Story Example

Mid-Level Solution Requirements Template Instructions

The SIMM Section 19B.3 Mid-Level Solution Requirements Template is an Excel tool agencies/state entities can use to document requirements for the PAL. The fields included in the Mid-Level Solution Requirements Template are required and must be included in an agency/state entity's requirement documentation submission. Agencies/state entities may utilize another requirement documentation format as long as the required fields are included in their requirements documentation submission. Additionally, agencies/state entities may include more fields than those provided in the Mid-Level Solution Requirements Template.

The Mid-Level Solution Requirements Template introduces a component of traceability that is initially developed as part of Stage 2 Alternatives Analysis and will be further elaborated in Stage 3 Solution Analysis. Traceability helps to ensure that what is delivered by the completed solution is neither more nor less than what was agreed to by the project stakeholders. See SIMM 17 for a sample Requirements Traceability Matrix and user instructions.

If using the Mid-Level Solution Requirements Template, enter the "Project Number" and "Agency/State Entity Name" on the **Instructions** tab. This will automatically populate each corresponding "Requirement Type" tab. Refer to the template's **Instructions** tab for specific steps to combine all requirement types onto one worksheet.

Enter Requirements – Use the *corresponding* tab for the "Requirement Type" (e.g., Functional Mandatory tab, Functional Desirable tab, Non-Functional Mandatory tab) to enter the mid-level solution requirements. The following information is required:

Objectives Reference – Enter the "Objective Number" from the Stage 1 Business Analysis Section 1.10 Business Problems or Opportunities and Objectives Table to reference each functional requirement to one of the objectives identified in the Stage 1 Business Analysis. This will show the linkage, or "traceability," of the requirements back to the project objectives.

Requirement Category – Enter the agency/state entity defined requirement category that aligns with the functional area (e.g., HR, IT, SYS).

Requirement Number – Enter the agency/state entity defined requirement number. This number will in most cases be used for traceability purposes.

Main Business Capability/Function – Enter the name of the business function which this requirement will help address. For example: Eligibility and Enrollment.

Sub Business Capability/Function – Enter the sub business capability/function that is expected to occur as a result of a main business capability/function. For example: Determine eligibility.

Business Process – Enter a brief description of the business process. The description should identify the event that triggers the business process, the series of business process activities, and the data manipulated by the business process. For example: Process Claim – This business process receives the original or adjusted claim information and validates that the required information has been completed.

Requirement – Enter the requirement that supports the main business and/or sub-business capability or functional needs and the corresponding objective.

Requirement Type – The requirement type (e.g., functional, non-functional, project/transition) will automatically populate based on the corresponding tab's requirement type. The requirement types are as follows:

Functional Requirements – Functional requirements represent the business objectives, needs and outcomes of all stakeholders. They should be organized and presented in context of and with a baseline business process/workflow that they describe. They provide a description of what an enabling solution should provide and specify essential details of a solution for stakeholders as a means to express and manage expectations. They describe actions and operations that the solution must be able to perform. They can describe services, reactions, and behaviors of the solution. They also describe information the solution will manage. The requirements should be expressed in business terms and should not include any technical references. The requirement should identify "what" is required to meet the business objective, not "how" the requirement will be implemented.

For example:

- The solution shall provide the functionality to list available plans and benefit designs online, via the internet.
- The solution shall provide on-line help features including:
  - How-to examples
  - An index of all provided features
  - A glossary of terms
  - System documentation as described in Section XX of RFP XX
  - Key command instructions
- The solution shall allow end users to print reports, text, tables, maps, and charts/graphs in hardcopy form, on end user's local or network printers.
- Edit errors shall provide user with range of correct values for the field in question.

Non-Functional Requirements – Non-functional requirements provide criteria to evaluate the operation of an enabling solution and primarily represent qualities of (expectations and characteristics) and constraints on (e.g., governmental regulations) the solution. They capture conditions that do not directly relate to the behavior or functionality of the solution, but rather describe environmental conditions of an effective solution or productive qualities of the solution. Mid-level non-functional requirements also define quality of service requirements, such as those relating to required capacity, speed, security, privacy, availability, response time, throughput, usability, and the information architecture and presentation of the user interfaces. Mid-level non-functional requirements could include the following:

- Quality Requirements (include 'abilities') –
  - Reusability
  - Maintainability
  - Reliability
  - Security
  - Portability

  For Example:
  - Solution shall require authorized users to change their password monthly.
  - Interruptions of system availability for planned maintenance shall be scheduled.
  - Data fields specified in Form XX shall be consistent with the data element definitions specified in the data dictionary.
  - Logical and physical access to the system will be restricted to authorized users.
  - Password-based authentication will authorize users to the system.

- Human Factors (include required characteristics for the outcomes of interaction with human users) –
  - Performance
  - Usability
  - Availability
  - Efficiency
  - Safety

  For Example:
  - Solution shall notify the user when a new is new record is submitted.
  - Solution shall support all concurrent users, without degradation of system performance and/or functionality.
  - Solution shall provide menu-driven navigation.
  - Browser-based users will gain access to the system via a single login.
  - Solution shall provide simultaneous on-line query access.

- Design Constraints (requirements that limit the options open to a solution designer) –
  - Standards
  - Policies
  - Data center options
  - Interfaces

  For Example:
  - System shall encrypt all data while in transit and at rest.
  - End users shall perform queries against the database using SAS Business Analytics software.
  - System shall provide a web-based interface.
  - System shall provide data access to the record level using Windows based graphical interface.
  - Provide data access for end users without the prior programming knowledge.

Project/Transition Requirements – Project/transition requirements describe capabilities that the solution must have in order to facilitate the transition from the current state of the

enterprise to a desired future state. Mid-level project/transition requirements are differentiated from other requirement types because they are usually temporary in nature and will not be needed once the transition is complete. They typically cover process requirements imposed through the contract, such as mandating a particular design method, administrative requirements, data conversion and migration from existing systems, interfaces, skill gaps that must be addressed, and other related changes required to reach the desired future state.

Mid-level project/transition requirements could include the following:

- Project Requirements
  - Compliance requirements
  - System Development Life Cycle (SDLC) or system element implementation process requirements
  - Project management and reporting

  For Example:

  - Contractor shall specify and follow an industry-standard SDLC methodology, such as Waterfall, or Rational Unified Process.
  - Contractor shall provide weekly status reports.
  - Contractor shall develop a Microsoft Project schedule, detailing all project tasks greater than 40 hours of effort.
- Transition Requirements
  - Data conversion and migration
  - Production turnover and transition (help desk, operations, application support)
  - User preparation and transition (training)
  - Customer preparation and transition (communications, data interchange)
  - Organizational changes
  - Infrastructure preparations

  For Example:

  - Contractor shall be responsible for loading all data supplied by the department into the new system.
  - Contractor shall be responsible for providing monthly Enterprise Resource Planning system training to a maximum of 20 users per class, for a period of 12 months.
  - Contractor shall provide on-line, hands-on use of the system as an essential part of training.
  - Contractor shall provide on-call telephone support and user-assistance.
- Operation and Support (requirements that specify the physical environment in which the system will operate and provisions for sustaining the operational effectiveness and use of the system) –

  For Example:

  - Contractor shall provide up to 2,000 hours each year of technical consultation and services for system maintenance.
  - Contractor shall provide sufficient licenses for 400 concurrent end users.
  - Contractor shall perform preventative maintenance and update the system in response to system defects.
  - Contractor shall provide on-call support 24 hours a day, seven days a week.

- Vendor Qualification Requirements
  - Experience of the vendor and its subcontractors
  - Performance Bonds and Insurance
  - Provision of audited financial statements

  For Example:

  - Contractor must have completed two (2) projects within the past five (5) years with primary responsibility for implementing similar business functions identified in this solicitation.
  - Contractor shall provide resumes and three references for all proposed staff that shall fill the positions detailed in the Contractor Staffing Requirements section of this RFP.
  - Contractors' proposed Project Manager shall be a certified Project Management Professional by the Project Management Institute.

Priority: The priority of each functional requirement will automatically populate based on the corresponding tab's requirement priority type, as follows:

- Mandatory – "Must have" requirements that are critical to the functionality of the solution.
- Desirable – "Nice to have" features – features that are not critical to the functionality of the solution.

Business Owner/Stakeholder: Specify a business owner/stakeholder or stakeholder group that benefits from the implementation of the requirement. This business owner/stakeholder will become the owner of the requirement to ensure that the requirement is implemented correctly in the system. The business owner/stakeholder identified should align with Stage 1 Business Analysis.

Epics/User Stories (Samples):

Agile methodology guidelines

GSA User Story Guidelines

User Story Example

Atlassian Epics Sample

Atlassian User Stories Sample

Kanbanize Epics and User Stories Example

2.5 Assumptions and Constraints

To be able to identify the solution requirements, a certain number of assumptions and constraints are necessary. By definition, an assumption is something that is accepted as true or is certain to happen, without proof. Constraints place limits or conditions on the proposed project. Therefore, the list of assumptions and constraints should be reasonable and, if possible, be supported by quantifiable information. Assumptions and constraints should be realistic and accurate; otherwise, the overall credibility of the business case can be negatively affected.

Assumptions: Enter each assumption and constraint.

Examples of assumptions include:

- **Staff working hours are set to an 8:00 am to 5:00 pm schedule.**
- **Dedicated staff will cross train one another.**
- **Procurement timeline will be developed and agreed upon between CDT, STP, and the department.**
- **Project will continue to be a high priority for the department and agency.**
- **Technology is available to create a solution which meets the program needs.**

Description/Potential Impact: Describe the assumption and the potential impact on the proposed project if not addressed.

This narrative should identify how the assumption was identified. Include how any financial impacts were identified and determined.

Constraints: Enter each assumption and constraint.

Examples of constraints include:

- **Project Implementation has a hard deadline.**
- **Privacy considerations.**
- **Details for financial analysis will be estimated.**
- **Subject Matter Expert resources are available to the project.**

Description/Potential Impact: Describe the constraint and the potential impact on the proposed project if not addressed.

This narrative should identify how the constraint was identified. Include how any financial impacts were identified and determined.

2.6 Dependencies

Dependencies are elements or relationships in a project reliant on something else occurring before the function, service, interface, task, or action can begin or continue. Dependencies may involve another project (e.g., a program in a project is waiting on deliverables or staff from another project before it can continue) or be reliant on another area within a project (e.g., a team must complete a deliverable before another team can begin their task). Dependencies should be related to the business need or solution requirements and not a specific option.

Dependency Element: Enter the element with dependencies on another function, service, interface, task, or action before it may begin or continue.

The element specifies the function, service, task, or action that is dependent on something else before it may begin or continue.

Examples of dependencies include:

- **Vendor will train users on access and navigation of the solution.**

- **Funding will be available for the duration of the project.**
- **Data Migration cleanup and validation required.**
- **User Authentication will rely on Active Directory.**
- **Hiring a consultant as Project Manager.**

Dependency Description: Enter the description for the element.

The dependency's element description should highlight the manner a particular initiative or entity (internal or external) associated with the proposed project relies on a specific enabling function, service, interface, task, or action to begin or continue. For example, data preparation for migration may be dependent on documenting both the business rules and current data dictionary descriptions. Therefore, the data preparation for migration is dependent on the completion of these tasks before it can begin.

2.7 Market Research

Agencies/state entities are required to perform market research to collect information and analyze the capabilities of vendors in the existing market. Market research determines whether the business needs identified in this proposal can be met by products or services available in the marketplace; whether commercial practices regarding customizing, or modifying products or tailoring services are available to meet the business needs or objectives of the proposal. Market research is also used to determine how many vendors, if any, can provide solutions to the business problem or opportunity of the proposal. This can shape the procurement strategy, which helps determine the type and content of the product description or statement of work, develops the support strategy, refines requirements, and identifies evaluation factors used for the solicitation. Market research should be aligned with the proposal's business, technical and functional objectives, including cost estimates.

Note*: Refer to the Market Research Guidelines for additional guidance on performing market research located at: https://cdt.ca.gov/wp-content/uploads/2019/08/Market-Research-Guidelines.pdf*

2.7.1 Project Management Methodology

Identify the current project management methodology approach for the project execution.

2.7.2 Procurement Approach Recommended

Please identify the approach for procurement here. This approach method will determine the Procurement timeline and how it fits into the remaining PAL process. Please reach out to your CDT PAO representative and STP representative if you are unable to answer this.

2.7.3 Market Research Approach

Approach Used to Perform Market Research: Detail the approach in a narrative format used to conduct market research. Include the following information in this narrative such as methodologies used, time spent, and start/end dates.

Provide a concise narrative description of the approach used to perform market research. The narrative should include a brief description of the following:

- How were results analyzed?

- Who was involved in the analysis of results (technical staff, key stakeholders, business sponsors, etc.)?
- How have results affected requirements development?
- How have results influenced procurement methodologies?
- Alignment of results with the recommended alternative.

Refer to State Contracting Manual (SCM) Chapter 13, Market Research Guidelines for general descriptions of the methodologies listed:

- Request for Information (RFI)
- Internet Research
- Vendor Forums/Presentations
- Collaboration with other agencies/state entities or governmental entities
- Trade shows
- Published literature
- Leveraged Agreements
- Other. Specify methodology used

Time spent conducting market research: Give a cumulative timeframe that the agency/state entity spent conducting market research, such as:

- 1 Month
- 6 Months
- 1 Year
- More than 1 Year
- 4 Years

Date market research was started: Include the date market research activities began.

Date all market research was completed: Include the date all market research activities were completed.

2.7.4 Market Research Artifacts

Attach all market research artifacts used to conduct research. This includes items such as a Request for Information (RFI), internet research, collaboration with other state or federal government entities, and reaching out to existing partners.

2.8 Viable Alternative Solutions

The CDT expects agencies/state entities to conduct a thorough analysis of all feasible alternatives that will meet the proposal's objectives and requirements. Agencies/state entities must consider **at least three alternative solutions**. The "do nothing" alternative will not count toward the three minimum alternative requirements.

Proposals submitted with less than three alternatives considered will not be accepted without a detailed discussion describing the specific research undertaken to justify why no other possible alternative exists.

2.8.1 Viable Alternative Solution #1

The agency/state entity will designate only **one** alternative solution as the "#1" solution based on an analysis of which alternative best satisfies the previously defined objectives and requirements. All other alternatives will be designated by the agency/state entity as a "Viable Solution."

Name: Enter the name for the alternative solution considered.

Description: Enter a brief narrative that describes the alternative, including what the alternative is and why the alternative was considered.

Why is this viable solution #1? Please explain. Enter a narrative describing why this solution was chosen to be the first selected solution. Please include benefits and advantages as well as detriments and disadvantages against the other viable solutions.

Approach: Select Yes for each approach's method to address the problems and meet the objectives and requirements. Select No for approaches not used.

- Increase staff – new or existing capabilities
- Modify the existing business process or create a new business process
- Reduce the services or level of services provided
- Utilize new or increased contracted services
- Enhance the existing IT system
- Modify Statute/Policy/Regulations
  - Specify: Explain the changes and the existing item being modified.
- Create a new IT system
- Other. Specify in space provided

Architecture Information: The agency/state entity business and technical teams will collaborate to complete the information contained within the Architecture Information. The business team will complete, or provide to the technical team, the business processes for the proposed solution. The technical team will complete, or provide to the business team, the technical-related items (e.g., application, system, or component; COTS/SaaS/Cloud Technology or custom solution; runtime environment; system interfaces; data center location; and, security) for the proposed alternative solution. The Architecture Information should align with Section 2.3 Current Business Environment and 2.3 Technical Context.

Document the business processes and supporting technology of the alternative solution. For each business process identified in Stage 1 Business Analysis Section 1.5 Business Background, provide the following:

Business Function/Process(es): Enter the business process name as referenced by the Agency/state entity. If many business processes are grouped under business functions (particularly for large systems), identify the respective business function.

TIP: Copy and paste to add business processes with the same application, system, or component; COTS/Cloud Technology or custom solution; runtime environment; system interfaces, data center location; and security.

Application, System, or Component: Enter the name of the application, system or component that supports the associated business process.

TIP: Copy and paste to add an application, system or component as needed.

COTS/SaaS/Cloud Technology or Custom: Select either “Commercial off-the-shelf (COTS)/Software as a Service (SaaS)/Cloud Technology” or “Custom solution” to identify the type of application, system or component used. For a COTS/Cloud Technology product, provide the name of the COTS or Cloud Technology product utilized in the system. For a custom solution, enter the primary technology used to build the system (e.g., .NET, Java).

- COTS/SaaS/Cloud Technology product – Typically, a ready-made computer hardware or software product for specific uses and available for sale to the general public. COTS products are designed to be installed without requiring custom development. For example, Microsoft Office is a COTS product that is a packaged software solution for businesses and individuals. The Federal Acquisition Regulation (FAR) defines the rules for COTS products.

- Custom solution – Typically, computer software developed for a specific customer to accommodate the customer's particular requirements, preferences, and expectations.

System Interfaces (new and existing): Enter the name(s) of system(s) that exchange data with the alternative system using interface files, web services, etc. Identify systems within scope of the proposed project that interface with each other. Also identify systems outside the scope of the proposed project that interface with the baseline systems. Provide a brief description of the purpose of each interface. If the system exchanges data with other entities, specify the name of the entity. Examples include but are not limited to the following:

- Federal partners
- Local city/county partners
- State agency entity partners
- Judicial branch
- Universities
- Researchers

Data Center Location of the To-be Solution: Select the location of the data center where the alternative system will be hosted.

- State Data Center: A data center operated by the CDT, Office of Technology Services (OTech).
- Agency/State Entity Data Center: A data center independently operated by an agency/state entity.
- Commercial Data Center: A data center operated by a solution provider or vendor contracted by the agency/state entity.
- Other: If not one of the above, identify the location and owner of the data center where the alternative system will be hosted.

Security: Indicate the security and privacy characteristics of the alternative system.

Access: Select Yes or No for each access type to identify who is authorized to access the current system:

- Public: Select Yes if the alternative system will be accessible to public parties with or without restricted access.
- Internal State staff: Select Yes if the alternative system will be accessible to internal state staff with or without restricted access.
- External State staff: Select Yes if the alternative system will be accessible to state staff from other agencies/state entities, with or without restricted access.
    - Other. Specify who else is authorized to access the alternative system.

Type of Information: Select Yes or No for each to identify the type of information that requires protection. See the SAM Section 5305.5 for more information.

- Personal: Select Yes if personally identifiable information (e.g., social security numbers, demographic information) will be collected, processed and/or presented by the alternative system.
- Health: Select Yes if diagnosis, treatment, provider, insurance, or billing information will be collected, processed and/or presented by the alternative system.
- Tax: Select Yes if IRS safeguards or state or local tax information policies (similar to the Federal IRS safeguards) are required to protect information contained in state or local tax submissions.
- Financial: Select Yes if confidential or sensitive financial information will be maintained (e.g., payment processing, salaries, budget, credit card numbers, contract amounts).
- Legal: Select Yes if confidential or sensitive legal information will be maintained (e.g., arrest records, court records, incarceration records, contracts, lawsuits, legal documents).
- Confidential: Select Yes if other types of confidential or sensitive information will be maintained by the system (e.g., business trade secrets, investigations, enforcement actions).
- Other: Specify the type of information that requires protection.

Protective Measures: Select Yes or No to identify the protective measures used to protect information.

- Technical Security: Select Yes if hardware and software security measures (e.g., firewalls, virus protection, intrusion detection/prevention) will be used to protect the networks, servers, workstations, and other devices in the infrastructure.
- Identity Authorization and Authentication: Select Yes if the alternative system will be required to restrict access to either state employees and/or to the public.
- Physical Security: Select Yes if servers and network devices will be secured with environmental security measures (e.g., door locks, surveillance equipment).
- Backup and Recovery (Technology Recovery): Select Yes if data will be backed up and stored offsite.
- Other, specify: If other, specify how the information will be currently protected.

Cost Summary of Alternative Solution: Enter each part of the cost of this solution. These costs must match the Financial Analysis Worksheet, submitted in Section 2.12, for the Proposed Alternative Solution #1 in the Summary Tab.

2.8.2 Viable Alternative Solution #2

The agency/state entity will designate only **one** alternative solution as the "#1" solution based on an analysis of which alternative best satisfies the previously defined objectives and requirements. All other alternatives will be designated by the agency/state entity as a "Viable Solution #X."

Name: Enter the name for the alternative solution considered.

Description: Enter a brief narrative that describes the alternative, including what the alternative is and why the alternative was considered.

Why is this a viable solution? Please explain. Enter a narrative describing why this solution was chosen to be viable. Please include benefits and advantages as well as detriments and disadvantages against the other viable solutions.

Approach: Select Yes for each approach's method to address the problems and meet the objectives and requirements. Select No for approaches not used.

- Increase staff – new or existing capabilities
- Modify the existing business process or create a new business process
- Reduce the services or level of services provided
- Utilize new or increased contracted services
- Enhance the existing IT system
- Modify Statute/Policy/Regulations
  - Specify: Explain the changes and the existing item being modified.
- Create a new IT system
- Other. Specify in space provided

Architecture Information: The agency/state entity business and technical teams will collaborate to complete the information contained within the Architecture Information. The business team will complete, or provide to the technical team, the business processes for the proposed solution. The technical team will complete, or provide to the business team, the technical-related items (e.g., application, system, or component; COTS/SaaS/Cloud Technology or custom solution; runtime environment; system interfaces; data center location; and, security) for the proposed alternative solution. The Architecture Information should align with Section 2.3 Current Business Environment and 2.3 Technical Context.

Document the business processes and supporting technology of the alternative solution. For each business process identified in Stage 1 Business Analysis Section 1.5 Business Background, provide the following:

Business Function/Process(es): Enter the business process name as referenced by the Agency/state entity. If many business processes are grouped under business functions (particularly for large systems), identify the respective business function.

TIP: Copy and paste to add business processes with the same application, system, or component; COTS/Cloud Technology or custom solution; runtime environment; system interfaces, data center location; and security.

Application, System, or Component: Enter the name of the application, system or component that supports the associated business process.

TIP: Copy and paste to add an application, system or component as needed.

COTS/SaaS/Cloud Technology or Custom: Select either "Commercial off-the-shelf (COTS)/Software as a Service (SaaS)/Cloud Technology" or "Custom solution" to identify the type of application, system or component used. For a COTS/Cloud Technology product, provide the name of the COTS or Cloud Technology product utilized in the system. For a custom solution, enter the primary technology used to build the system (e.g., .NET, Java).

- COTS/SaaS/Cloud Technology product – Typically, a ready-made computer hardware or software product for specific uses and available for sale to the general public. COTS products are designed to be installed without requiring custom development. For example, Microsoft Office is a COTS product that is a packaged software solution for businesses and individuals. The Federal Acquisition Regulation (FAR) defines the rules for COTS products.

- Custom solution – Typically, computer software developed for a specific customer to accommodate the customer's particular requirements, preferences, and expectations.

System Interfaces (new and existing): Enter the name(s) of system(s) that exchange data with the alternative system using interface files, web services, etc. Identify systems within scope of the proposed project that interface with each other. Also identify systems outside the scope of the proposed project that interface with the baseline systems. Provide a brief description of the purpose of each interface. If the system exchanges data with other entities, specify the name of the entity. Examples include but are not limited to the following:

- Federal partners
- Local city/county partners
- State agency entity partners
- Judicial branch
- Universities
- Researchers

Data Center Location of the To-be Solution: Select the location of the data center where the alternative system will be hosted.

- State Data Center: A data center operated by the CDT, Office of Technology Services (OTech).
- Agency/State Entity Data Center: A data center independently operated by an agency/state entity.
- Commercial Data Center: A data center operated by a solution provider or vendor contracted by the agency/state entity.
- Other: If not one of the above, identify the location and owner of the data center where the alternative system will be hosted.

Security: Indicate the security and privacy characteristics of the alternative system.

Access: Select Yes or No for each access type to identify who is authorized to access the current system:

- Public: Select Yes if the alternative system will be accessible to public parties with or without restricted access.
- Internal State staff: Select Yes if the alternative system will be accessible to internal state staff with or without restricted access.
- External State staff: Select Yes if the alternative system will be accessible to state staff from other agencies/state entities, with or without restricted access.
    - Other. Specify who else is authorized to access the alternative system.

Type of Information: Select Yes or No for each to identify the type of information that requires protection. See the SAM Section 5305.5 for more information.

- Personal: Select Yes if personally identifiable information (e.g., social security numbers, demographic information) will be collected, processed and/or presented by the alternative system.
- Health: Select Yes if diagnosis, treatment, provider, insurance, or billing information will be collected, processed and/or presented by the alternative system.
- Tax: Select Yes if IRS safeguards or state or local tax information policies (similar to the Federal IRS safeguards) are required to protect information contained in state or local tax submissions.
- Financial: Select Yes if confidential or sensitive financial information will be maintained (e.g., payment processing, salaries, budget, credit card numbers, contract amounts).
- Legal: Select Yes if confidential or sensitive legal information will be maintained (e.g., arrest records, court records, incarceration records, contracts, lawsuits, legal documents).
- Confidential: Select Yes if other types of confidential or sensitive information will be maintained by the system (e.g., business trade secrets, investigations, enforcement actions).
- Other: Specify the type of information that requires protection.

Protective Measures: Select Yes or No to identify the protective measures used to protect information.

- Technical Security: Select Yes if hardware and software security measures (e.g., firewalls, virus protection, intrusion detection/prevention) will be used to protect the networks, servers, workstations, and other devices in the infrastructure.
- Identity Authorization and Authentication: Select Yes if the alternative system will be required to restrict access to either state employees and/or to the public.
- Physical Security: Select Yes if servers and network devices will be secured with environmental security measures (e.g., door locks, surveillance equipment).
- Backup and Recovery (Technology Recovery): Select Yes if data will be backed up and stored offsite.
- Other, specify: If other, specify how the information will be currently protected.

Cost Summary of Alternative Solution: Enter the cost of this solution as identified in the Financial Analysis Worksheet, Summary tab.

2.8.3 Viable Alternative Solution #3

The agency/state entity will designate only **one** alternative solution as the “#1” solution based on an analysis of which alternative best satisfies the previously defined objectives and requirements. All

other alternatives will be designated by the agency/state entity as a “Viable Solution #X.” If you have more than 3 Alternative Solutions, copy/paste this section to add as many alternatives as needed.

Name: Enter the name for the alternative solution considered.

Description: Enter a brief narrative that describes the alternative, including what the alternative is and why the alternative was considered.

Why is this a viable solution? Please explain. Enter a narrative describing why this solution was chosen to be viable. Please include benefits and advantages as well as detriments and disadvantages against the other viable solutions.

Approach: Select Yes for each approach’s method to address the problems and meet the objectives and requirements. Select No for approaches not used.

- Increase staff – new or existing capabilities
- Modify the existing business process or create a new business process
- Reduce the services or level of services provided
- Utilize new or increased contracted services
- Enhance the existing IT system
- Modify Statute/Policy/Regulations
  - Specify: Explain the changes and the existing item being modified.
- Create a new IT system
- Other. Specify in space provided

Architecture Information: The agency/state entity business and technical teams will collaborate to complete the information contained within the Architecture Information. The business team will complete, or provide to the technical team, the business processes for the proposed solution. The technical team will complete, or provide to the business team, the technical-related items (e.g., application, system, or component; COTS/SaaS/Cloud Technology or custom solution; runtime environment; system interfaces; data center location; and, security) for the proposed alternative solution. The Architecture Information should align with Section 2.3 Current Business Environment and 2.3 Technical Context.

Document the business processes and supporting technology of the alternative solution. For each business process identified in Stage 1 Business Analysis Section 1.5 Business Background, provide the following:

Business Function/Process(es): Enter the business process name as referenced by the Agency/state entity. If many business processes are grouped under business functions (particularly for large systems), identify the respective business function.

TIP: Copy and paste to add business processes with the same application, system, or component; COTS/Cloud Technology or custom solution; runtime environment; system interfaces, data center location; and security.

Application, System, or Component: Enter the name of the application, system or component that supports the associated business process.

TIP: Copy and paste to add an application, system or component as needed.

COTS/SaaS/Cloud Technology or Custom: Select either “Commercial off-the-shelf (COTS)/Software as a Service (SaaS)/Cloud Technology” or “Custom solution” to identify the type of application, system or component used. For a COTS/Cloud Technology product, provide the name of the COTS or Cloud Technology product utilized in the system. For a custom solution, enter the primary technology used to build the system (e.g., .NET, Java).

- COTS/SaaS/Cloud Technology product – Typically, a ready-made computer hardware or software product for specific uses and available for sale to the general public. COTS products are designed to be installed without requiring custom development. For example, Microsoft Office is a COTS product that is a packaged software solution for businesses and individuals. The Federal Acquisition Regulation (FAR) defines the rules for COTS products.

- Custom solution – Typically, computer software developed for a specific customer to accommodate the customer's particular requirements, preferences, and expectations.

System Interfaces (new and existing): Enter the name(s) of system(s) that exchange data with the alternative system using interface files, web services, etc. Identify systems within scope of the proposed project that interface with each other. Also identify systems outside the scope of the proposed project that interface with the baseline systems. Provide a brief description of the purpose of each interface. If the system exchanges data with other entities, specify the name of the entity. Examples include but are not limited to the following:

- Federal partners
- Local city/county partners
- State agency entity partners
- Judicial branch
- Universities
- Researchers

Data Center Location of the To-be Solution: Select the location of the data center where the alternative system will be hosted.

- State Data Center: A data center operated by the CDT, Office of Technology Services (OTech).
- Agency/State Entity Data Center: A data center independently operated by an agency/state entity.
- Commercial Data Center: A data center operated by a solution provider or vendor contracted by the agency/state entity.
- Other: If not one of the above, identify the location and owner of the data center where the alternative system will be hosted.

Security: Indicate the security and privacy characteristics of the alternative system.

Access: Select Yes or No for each access type to identify who is authorized to access the current system:

- Public: Select Yes if the alternative system will be accessible to public parties with or without restricted access.

- Internal State staff: Select Yes if the alternative system will be accessible to internal state staff with or without restricted access.
- External State staff: Select Yes if the alternative system will be accessible to state staff from other agencies/state entities, with or without restricted access.
    - Other. Specify who else is authorized to access the alternative system.

Type of Information: Select Yes or No for each to identify the type of information that requires protection. See the SAM Section 5305.5 for more information.

- Personal: Select Yes if personally identifiable information (e.g., social security numbers, demographic information) will be collected, processed and/or presented by the alternative system.
- Health: Select Yes if diagnosis, treatment, provider, insurance, or billing information will be collected, processed and/or presented by the alternative system.
- Tax: Select Yes if IRS safeguards or state or local tax information policies (similar to the Federal IRS safeguards) are required to protect information contained in state or local tax submissions.
- Financial: Select Yes if confidential or sensitive financial information will be maintained (e.g., payment processing, salaries, budget, credit card numbers, contract amounts).
- Legal: Select Yes if confidential or sensitive legal information will be maintained (e.g., arrest records, court records, incarceration records, contracts, lawsuits, legal documents).
- Confidential: Select Yes if other types of confidential or sensitive information will be maintained by the system (e.g., business trade secrets, investigations, enforcement actions).
- Other: Specify the type of information that requires protection.

Protective Measures: Select Yes or No to identify the protective measures used to protect information.

- Technical Security: Select Yes if hardware and software security measures (e.g., firewalls, virus protection, intrusion detection/prevention) will be used to protect the networks, servers, workstations, and other devices in the infrastructure.
- Identity Authorization and Authentication: Select Yes if the alternative system will be required to restrict access to either state employees and/or to the public.
- Physical Security: Select Yes if servers and network devices will be secured with environmental security measures (e.g., door locks, surveillance equipment).
- Backup and Recovery (Technology Recovery): Select Yes if data will be backed up and stored offsite.
- Other, specify: If other, specify how the information will be currently protected.

Cost Summary of Alternative Solution: Enter the cost of this solution as identified in the Financial Analysis Worksheet, Summary tab.

2.9 Current Project Organization

Project planning is the process of identifying how and when labor needs will be met to ensure that the proposed project has sufficient staff with the appropriate skill sets and experience. Project planning will identify and document project roles, responsibilities and reporting relationships and result in the creation of a Staff Management Plan (PMBOK®) or Human Resource Management Plan (CA-PMM).

In the following sections, provide a concise description of the approach to staffing the proposed project including contingencies for business/program, IT, or administrative areas to maintain ongoing operations in conjunction with the proposed project. These narratives should address both the resource needs to perform the work required in Stages 3 and 4 of the PAL, excepting where specified, including subject matter experts identified, and the impact the project will have on existing operations and mitigation strategies throughout the life of the project. This narrative should also identify how the agency/state entity will supply sufficient numbers of knowledgeable internal resources for projects that are anticipated to have a strong dependency on vendors.

2.9.1 Project Organization Chart

Attachment: Attach organization charts in PDF to show the agency/state entity and proposed project reporting relationships for all parties involved in the project.

To better assess this project's impact on the agency/state entity, the following charts/information is required:

Project Organization Chart

Project Team, including number and classification of team members. Organization chart should depict all of the state and vendor staff (if known prior to Stage 3 Solution Development) involved at any time in the project lifecycle. State staff identified on the organization chart should align with the new and existing staff identified in the FAWs.

i. Agency/state entity project management staff, including the Project Manager and Project Management Office (PMO) support staff.

ii. Agency/state entity business staff that will participate in the project, such as the Program Manager, program analysts, and subject matter experts.

iii. Agency/state entity information technology staff, including architects, systems analysts, software developers, quality assurance analysts, and requirements analysts.

iv. Vendor staff (if contracted or planned to contract) if known.

Business Sponsors and Key Stakeholders identified in Stage 1 Business Analysis.

Procurement Organization Chart

Procurement Team, including number and classification of procurement team members. Organization chart should depict all of the state and vendor staff (if known) involved during Stage 3 Solution Development and Stage 4 Project Readiness and Approval. State staff identified on the organization chart should align with the new and existing staff identified in the FAWs.

v. Agency/state entity procurement staff, including the Procurement Official, Backup Procurement Official, Procurement Manager, Contract Manager, Legal Reviewer, Information Security Officer Reviewer, Budget Manager/Reviewer.

vi. Agency/state entity project management staff, including the Project Manager and PMO support staff.

vii. Agency/state entity business staff that will participate in the procurement effort, such as the subject matter experts and evaluation team members.

viii. Agency/state entity information technology staff, including architects, systems analysts, quality assurance, and requirements analysts.

ix. Vendor staff (if contracted or planned to contract).

Business Sponsors and Key Stakeholders identified in Stage 1 Business Analysis.

Impacted Program(s) Organization Chart

Business Unit(s) and hierarchy tied back to Sponsor(s).

Information Technology Organization Chart

Per Government Code 11545, all IT personnel must report to CIO. This org chart must show all IT Classifications in the department.

Agency/State Entity Organization Chart

High level chart showing Executive Sponsor(s) in relation to Department Director and others.

2.9.2 Organization Structure

Is the department running this project as a matrixed or projectized organization? Projectized organization structure will have nearly all resources dedicated to the project full-time. Projectized structure will have resources reporting directly to the project's leadership team. Matrixed organization structure will have most resources dedicated less than full-time to the project. These resources will typically report to their original work areas and the project team leads as time will be split between the project and normal duties.

Staffing Organization

In each of the following sections, provide a concise description of the approach to staffing the proposed project including contingencies for business/program, IT, or administrative areas to maintain ongoing operations in conjunction with the proposed project.

2.9.1 Administrative

Describe the capacity and capability of administrative resources needed to maintain ongoing operations of the agency/state entity in conjunction with proposed project workload. This narrative should include the experience level of procurement, contract management and budget staff.

2.9.2 Business Program

Describe the capacity and capability of existing business program resources needed to maintain the business operations of the agency/state entity's business programs that will be impacted by this proposal. This narrative should identify how the agency/state entity will maintain ongoing program operations in conjunction with proposed project workload. If changes to business processes were identified in the Stage 1 Business Analysis, the narrative should also identify business program resources needed to perform business process reengineering activities.

2.9.3 Information Technology

Describe the capacity and capability of existing IT resources to both support this proposal and maintain existing responsibilities. This narrative should identify how the agency/state entity will maintain ongoing operations while the proposed project or any other initiative is underway.

2.9.4 Testing

Describe the capacity and capability of the agency/state entity's testing program and resources that will support all stages of testing (system, integration, security, performance, regression, user, etc.). This narrative should identify the dedicated resources to be assigned to support testing and adequately describe the skills and experience of these resources.

2.9.5 Data Conversion/Migration

If this proposal will require data conversion/migration activities, provide a brief description of the agency/state entity's plan for data conversion/migration. Describe the capacity and capability of the agency/state entity's resources that will support this effort.

2.9.6 Training

Describe the capacity and capability of training needed to support this proposal. This narrative should identify any business disruption and customer impacts which are anticipated to result with this proposal and include a description of the resources, processes, and methodologies in place to provide training services to mitigate any disruption.

2.9.7 Organizational Change Management

Describe the capacity and capability of organizational change management needed to support this proposal. This narrative should identify any business disruption and customer impacts which are anticipated to result with this proposal and include a description of the resources, processes, and methodologies in place to organizational change management services to mitigate any disruption.

2.9.8 Resource Capacity/Skills/Knowledge for Stage 3 Solution Development

Stage 3 Solution Development will require business program knowledge, technical knowledge, and procurement knowledge to effectively develop requirements, evaluation criteria, and contract deliverables. Describe the capacity, skill, and knowledge of the agency/state entity's procurement program and resources that will support the procurement effort (solicitation development, bidding, evaluation, contract award, etc.). This narrative should adequately describe the skills and experience of these resources that will be assigned to support procurement activities. The narrative should also address the following:

- Does the agency/state entity's governance framework include procurement related decision-making in addition to project decision-making?
- Does the agency/state entity's procurement office have experience using the proposed procurement methodologies identified in section 2.11.3 Procurement and Staffing Strategy?
- Does the agency/state entity's procurement office have experience using the STP Streamlined Template?
- Is the agency/state entity's procurement office familiar with protest types or use of Public Contract Code (PCC) 6611?

2.10 Project Management

This section has been split from current project organization. It covers the Project Management Risk Assessment document update as well as the Project Management Plans required to be submitted for PAL.

2.10.1 Project Management Risk Assessment

The Project Management Risk Assessment aids in assessing the maturity of an organization as a whole and their ability to carry out projects. This model will evaluate such elements as:

- Organizational commitment to a well-defined, mature project management process
- Existence of predicated management commitment, functions, and systems
- Competence of participants in any project management endeavor
- Organizational project management environment (e.g., tools, infrastructure) and how well these are integrated
- Measurement metrics in the organization and how well they are used and any applicable past performance
- Organization's continuous improvement process

This assessment is to be completed by the agency/state entity as part of the Stage 2 Alternatives Analysis and verified by the CDT during the Gate 2 collaborative review meeting. The results of the assessment may be evaluated by the California Project Management Office solely to identify potential service offerings.

Complete the Project Management Risk Assessment (located in SIMM Section 45 Appendix A) to determine the agency/state entity's Project Management Risk Assessment score. (Refer to SIMM Section 45 Appendix B for Project Management Risk Assessment preparation instructions).

Note*: Only complete the questions identified as Stage 1 and Stage 2 in the "Required Stage" column*.

Updated Project Management Risk Score: Enter the score.

Attachment: **Attach** an electronic copy of the updated Project Management Risk Assessment to your email submission.

2.10.2 Project Charter

Indicate the status of the project charter. Select "Yes" if the plan/artifact is complete, approved by the designated agency/state entity authority, and available for CDT review. Select "No" if the plan/artifact is under development, pending review/approval or not yet started and provide the status in the space provided. Select "Not Applicable" if the plan/artifact is not needed for the proposed project and provide an explanation in the space provided.

2.10.3 Project Management Planning

Indicate the status of the following project management plans or project artifacts. Select "Yes" if the plan/artifact is completed to the required level, approved by the designated agency/state entity authority (for plans marked "Approved"), and available for CDT review. Select "No" if the plan/artifact is under development, pending review/approval or not yet started and provide the status in the space provided. Select "Not Applicable" if the plan/artifact is not needed for the proposed project and provide an explanation in the space provided.

A list of required plans for each stage has been provided at the end of this instruction document.

Some plans may require additional pieces and have been detailed below which pieces are needed now. For example:

The Risk Management Plan requires submission of a Risk Log as well. The Risk Log and draft Risk Management Plan are due in Stage 2, however the completed Risk Management Plan will be required in Stage 3.

Low to Medium complexity and cost projects may discuss the option to submit a single Master Project Management Plan with your assigned Project Approval and Oversight Manager in leiu of individual plans.

Select the project management plan/artifact status (i.e., Yes, No or Not Applicable) for each of the following. If No or Not Applicable, provide the artifact status in the space provided:

- Scope Management Plan (Approved)
- Communication Management Plan (Approved)
- Schedule Management Plan (Approved)
- Procurement Management Plan (Approved)
- Requirements Management Plan (Approved)
- Stakeholder Management Plan (Draft)
- Governance Plan (Draft)
- Contract Management Plan (Draft)
- Resource Management Plan (Draft)
- Change Control Management Plan (Draft)
- Risk Management Plan (Draft and Risk Log)
- Issue and Action Item Management Plan (Draft and Issue Log)
- Cost Management Plan (Approved if planning BCP was approved)
    - The cost management plan must be submitted in an approved state for Stage 2 only if a planning BCP was approved for this effort. If a planning BCP was not submitted/approved, the Cost Management Plan will be required as an approved plan in Stage 4.

2.10.4 Project Roadmap (High-Level)

Attach a high-level Project Roadmap showing the remainder of the planning phase and transition into execution phase. Include any procurements that have been made for this project. This document will be updated for Stage 3 with the primary solicitation and any additional procurements.

Please enter the planning and project execution start dates in the following section. These dates must be shown on the roadmap.

Planning Start Date: Date the S1BA was started.

Estimated Planning End Date: Date Stage 4 is planning to be completed and project execution to start.

Estimated Project Start Date: Date project execution is expected to start.

Estimated Project End Date: Date project execution is expected to end and maintenance and operations efforts are expected to begin.

2.11 Data Conversion/Migration

Data conversion/migration is the process whereby data from its current sources (existing legacy systems, hardcopies, document images, etc.) is extracted, transformed, and loaded to a new system or format. Despite many lessons learned and best practices regarding data conversion/migration, many legacy system modernization project implementations fail to survey and prepare their legacy data prior to data conversion/migration, which oftentimes leads to the untimely discovery of dirty, duplicate, incomplete, and/or incorrect data. Consequently, new data conversion/migration tasks are identified that result in unanticipated project tasks, costs, resource needs, and schedule overruns.

Some of the key challenges for data conversion/migration include, but are not limited to:

- Lack of data governance
- Data conversion/migration planning was done without a clear understanding of the current environment, data architecture, and data quality of the existing legacy system
- Lack of staff expertise in data conversion/migration
- Lack of clearly established and realistic data conversion/migration requirements, key stakeholder expectations, and data conversion/migration acceptance criteria
- Lack of documented and/or refined data quality business rules and data dictionaries

Agencies/state entities can mitigate most of the known risks associated with data conversion/migration by proactively taking necessary steps to establish a clear understanding of the current environment, data architecture, and quality of the legacy data, and plan accordingly to get the data ready for conversion/migration before the data conversion/migration process begins.

If the agency/state entity has indicated in Section 2.3 that they have data that must be migrated to the new solution, then this section must be filled out.

Select the data conversion/migration activity status (i.e., Not Started, In Progress, Completed, or Not Applicable) for each of the following:

- Current Environment Analysis: The process of gathering and compiling information about the current environment to create a blueprint of the current legacy data architecture.

- Data Migration Plan: Identify the status of the data migration plan. Select “Completed” if the plan/artifact is completed to the required level, approved by the designated agency/state entity authority (for plans marked “Approved”), and available for CDT review. Select “In Progress” or “Not Started” if the plan/artifact is under development, pending review/approval or not yet started and provide the status in the space provided. Select “Not Applicable” if the plan/artifact is not needed for the proposed project and provide an explanation in the space provided.

- Data Profiling: The process of examining the data available in an existing data source (e.g., a database or a file) and collecting statistics and information about that data.

- Data Cleansing and Correction: Data cleansing (or data cleaning, data scrubbing) is the process of detecting and correcting (or removing) corrupt or inaccurate records from a record set, table, or database.

- Data Quality Assessment: The process of exposing technical and business data issues in order to plan data cleansing and data enrichment strategies.

- Data Quality Business Rules: A business rule expresses specific constraints on the creation, update, and removal of data within a business function. For example, the record of a purchase order may not be entered if the customer's credit rating is not adequate.

- Data Dictionaries: A data dictionary is a centralized repository of metadata or information about data, such as its relationship to other data, related business rules, its format and default values. Typically, a data dictionary provides a descriptive list of names, definitions, and attributes of data elements to be captured in an information system or database. It describes the definitions or the expected meaning and acceptable representation of data for use within a defined context of data elements within a dataset.

- Data Conversion/Migration Requirements: The conditions that must be met in order to deem the data conversion/migration successful.

If “Not Applicable” was selected for any of the data conversion/migration activities identified above, provide a brief explanation in the area provided as to why the activity is not applicable.

If “Not Started” was selected, provide a brief description of when the activity is planned to begin and the anticipated completion date.

Attachment: Attach completed data conversion/migration documentation, as applicable, to your email submission.

2.12 Financial Analysis Worksheets

Attachment: Attach the Financial Analysis Worksheet(s) (FAWs) for this proposal to your email submission.

The FAWs should document the cost and resource assumptions the agency/state entity made during the PAL. The FAWs provide a standard format for documenting the projected costs and financial benefits of the current method of operation and the proposed alternative. The worksheets are used to perform cost analyses of the full range of alternatives under consideration. See “SIMM 19F Financial Analysis Worksheets Preparation Instructions” for direction on how to complete the FAWs for the Stage 2 Alternatives Analysis.

Stage 2 Deliverables Summary

The following lists out the required deliverables for the Stage 2 Alternatives Analysis document to be submitted by the department. Please note that the CDT can receive emails containing a maximum of 25MB of attachments and 1000 files. If your email needs to be split, please let us know during the submission in case the emails are received out of order.

Stage 2 Deliverable List:

- Stage 2 Alternatives Analysis Document
- Project Executive Transmittal
- STP Procurement Assessment Form completed with Stage 2 information
- Current Business Environment Documentation
- Technical Context Documentation
- Data Governance Org Chart
- Data Governance Policies

- Data Governance Security policies, standards, and controls
- Data Governance Documented Policies, Accessibility Governance Plan, Governance Standards
- Security Categorization Impact Table
- Updated SIMM 45 Complexity Assessment
- Requirements and/or Outcomes Document
- Market Research Artifacts
- Conceptual Architecture for each viable alternative
- Project Organization Charts
- Updated SIMM 45 PM Risk Assessment
- High-Level Project Roadmap
- Financial Analysis Worksheets

Project Management Plans by Stage

The following plans are due during the Project Approval Lifecycle framework:

Stage 2:

- Scope Management Plan (Approved)
- Communication Management Plan (Approved)
- Schedule Management Plan (Approved)
- Procurement Management Plan (Approved)
- Requirements Management Plan (Approved)
- Stakeholder Management Plan (Draft)
- Governance Plan (Draft)
- Contract Management Plan (Draft)
- Resource Management Plan (Draft)
- Change Control Management Plan (Draft)
- Risk Management Plan (Draft and Risk Log)
- Issue and Action Item Management Plan (Draft and Issue Log)
- Cost Management Plan (Approved if planning BCP was approved)
    - The cost management plan must be submitted in an approved state for Stage 2 only if a planning BCP was approved for this effort. If a planning BCP was not submitted/approved, the Cost Management Plan will be required as an approved plan in Stage 4.

Stage 3:

- Project Management Plan (Draft)
- Risk Management Plan (Approved)
- Issue and Action Item Management Plan (Approved)
- Change Control Management Plan (Approved)
- Quality Management Plan (Approved)
- Testing Management Plan (Approved)
- Security Management Plan (Approved)
- Contract Management Plan (Updated Draft)
- Other plans (not required)

Stage 4:

- Contract Management Plan (Approved)
- Implementation Management Plan (Approved)
- Cost Management Plan (Approved)
- Configuration Management Plan (Draft)
- Data Management Plan (Draft)
- Maintenance and Operations Transition Management Plan (Draft)