Stage 2 Alternatives Analysis

California Department of Technology, SIMM 19B.2 (Ver. 3.0.8, 02/28/2022)

2.1 General Information

1. **Agency or State Entity Name:** Choose an item.

   If Agency/State entity is not in the list, enter here with the organization code.

   2667 – Office of the Inspector General, High-Speed Rail

2. **Proposal Name: OIG-HSR Audits and Reviews Software**

3. **Department of Technology Project Number (0000-000):** 2667-001

4. **S2AA Version Number:** Version 1

5. **CDT Billing Case Number:** RZX

6. Don't have a Case Number? Click here to get one.

2.2 Submittal Information

1. **Contact Information**

   Contact Name: Deputy Inspector General – Amanda Millen

   Contact Email: Amanda.Millen@oig.hsr.ca.gov

   Contact Phone: (916) 908-0922

2. **Submission Type: New Submission**

   If Withdraw, select Reason: Choose an item.

   If Other, specify reason here: Click or tap here to enter text.

   Sections Changed if an update or resubmission: (List all the sections that changed.)

   Click or tap here to enter text.

   Summary of Changes: (Summarize updates made.)

Click or tap here to enter text.

3. **Attach Project Approval Executive Transmittal to your email submission.**

4. **Attach Procurement Assessment Form to your email submission.**

5. **Conditions from Stage 1 Approval** (Enter any conditions from the Stage 1 Business Analysis approval letter issued by CDT or your AIO):

   Click or tap here to enter text.

2.3 Baseline Processes and Systems

1. **Current Business Environment (Describe the current business environment of which the effort will be understood and assessed in 500 words)**

   Currently, the Office of the Attorney General High Speed Rail (OIG-HSR) Audits and Reviews Division relies on basic Microsoft Office tools and manual workflows to conduct all audit and review activities enumerated in its statutory responsibilities. This includes:

   - Audit Planning and Execution: Work is planned and documented using Microsoft Word and Excel, with no centralized case management system or workflow engine. Teams manually track audit milestones, tasks, budgets, and due dates using spreadsheets.
   - Evidence Collection and Annotation: Supporting documentation is stored in shared folders within the Authority's file system. Evidence is not annotated within a centralized system. There is no tagging, indexing, or built-in linkage between findings and source documents.
   - Review and Supervision: Supervisory reviews are conducted via email, with reviewers inserting comments directly into Word documents. There is no formal approval workflow, version control, or system-enforced sign-off and document finalization processes.
   - Recommendations Management: Audit recommendations are recorded and memorialized in static Word tables. Tracking the Authority's implementation of recommendations is conducted manually, with status updates collected via email and stored in separate Excel files with no ability to link directly to supporting evidence provided by the Authority.
   - Reporting and Performance Monitoring: Reporting of audit findings, recommendations, timelines, and performance indicators (e.g., hours worked, audit duration, compliance with audit plans) is entirely manual. Staff hours are tracked using shared timesheets or emailed summaries, but cannot be recorded in a central location that tracks budget usage or variance (timekeeping system).
   - Continuing Professional Education (CPE) Tracking: Audit staff track CPE compliance manually, typically using shared Excel logs maintained by division management.

   This manual, fragmented approach increases administrative burden, risks loss of data integrity, and does not support required professional standards for evidence handling, versioning, and review documentation. It also inhibits OIG-HSR's ability to readily and reliably produce relevant

administrative data to budget control entities, such as the Department of Finance and Legislature.

Tip: Current Environment costs will be asked for in the Financial Analysis Worksheet to be completed in Section 2.12.

Attach relevant documentation to email submission (i.e., business process, workflow, problem analysis, user/stakeholder list, research findings). If these types of documents are not available, please indicate "Not Available," and explain the reason below:

Not available reason: Click or tap here to enter text.

2. **Technical Context (Describe the technical environment of which the effort will be understood and assessed in 500 words)**

The OIG-HSR currently operates without a dedicated audit management platform. Instead, the Audits and Reviews Division uses a collection of general-purpose tools hosted on Authority-controlled IT infrastructure to perform and document its audit activities. These baseline systems introduce technical and operational limitations that affect the integrity, efficiency, traceability, and independence of audit work.

Microsoft Office tools are the core applications used for planning audits, evaluating evidence and documenting findings, tracking recommendations, and capturing/memorializing supervisory review and sign-off. These tools are not designed to support collaborative workflows, do not readily allow or enforce version control, and cannot link evidence to findings in a structured and auditable way. As a result, staff currently rely on manual methods for inserting review comments and tracking completion of tasks or audit milestones, risking inconsistent documentation practices and creating a quality control situation inconsistent with professional standards for government auditing and reviews.

Shared network drives managed by the Authority serve as the primary repository for audit-related files and supporting documentation. These drives are accessible by Authority IT administrators, meaning that OIG-HSR cannot ensure that access to confidential audit materials is restricted solely to authorized staff until such time as the OIG-HSR is prepared to share its results. Conversely, even with shared network drives, the OIG-HSR lacks an efficient industry tool for collaborating with Authority management on the implementation status of OIG-HSR recommendations. Taken together, these shortcomings highlight additional need for the procurement of this software.

The technical environment is also constrained by the absence of any dedicated infrastructure or software configured to meet audit-specific standards, such as those issued by the Government Accountability Office (GAO) or the Association of Inspectors General. OIG-HSR does not currently operate any standalone system that supports role-based access control, automated workflows, secure digital evidence handling, or tracking of time, milestones, and performance metrics. Similarly, documenting compliance with relevant industry standards is not only riskier, but performed in a decentralized and cumbersome manner.

Attach relevant documentation to email submission (i.e., logical system environment diagrams, system interactions, business rules, application flows, stakeholder information, data flow charts). If these types of documents are not available, please indicate "Not Available," and explain the reason below:

Not available reason: N/A

3. **Data Management (Enter the information to indicate the data owner and custodian of the current system, if applicable.)**

   Data Owner Name: HSR-OIG

   Data Owner Title: Deputy Inspector General

   Data Owner Business Program area: Audits and Reviews Division

   Data Custodian Name: HSR-OIG

   Data Custodian Title: Deputy Inspector General

   Data Custodian Technical area: N/A

   Security - Data Classification and Categorization No

   Security - Privacy Threshold & Impact Assessment. No

4. **Existing Data Governance and Data**

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

      Answer (Unknown, Yes, No): No

      If data migration is required, please rate the quality of the data.

         Select data quality rating: Choose an item.

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

      Answer (Unknown, Yes, No): No

      If Yes, include the data governance organization chart as an attachment to your email submission.

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

      Answer (Unknown, Yes, No): Yes

      If Yes, include the data governance policies as an attachment to your email submission.

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

      Answer (Unknown, Yes, No): Yes

If Yes, attach the existing documented security policies, standards, and controls used to your email submission.

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

Answer (Unknown, Yes, No): Yes

If Yes, attach the existing documented policies, accessibility governance plan, and standards used to the email submission.

5. **Security Categorization Impact Table**

Consult the SIMM 5305-A Information Security Program Management Standard - Security Categorization Impact Table.

Attach a table (in PDF) that categorizes and classifies the agency/state entity's information assets related to this effort (e.g., paper and electronic records, automated files, databases requiring appropriate protection from unauthorized use, access, disclosure, modification, loss, or deletion). Each information asset for which the agency/state entity has ownership responsibility shall be inventoried and identified.

6. **Security Categorization Impact Table Summary**

Consult the SIMM 5305-A Information Security Program Management Standard - Security Categorization Impact Table to provide potential impact levels of the following areas:

Confidentiality: Low

Integrity: Low

Availability: Low

7. **Technical Complexity Score: 0.9**

(Attach a SIMM Section 45 Appendix C with Business and Technical Complexity sections completed to the email submission.)

2.4 Requirements and Outcomes

At this time in the project planning process, requirements and outcomes should be documented and indicative of how the Agency/State Entity envisions the final solution. This shall be accomplished either in the form of mid-level requirements (predictive methodology)/business capabilities or representative epics and user stories (adaptive methodology) that will become part of the product backlog. The requirements or representative epics and user stories must tie back to the Objectives detailed in the Stage 1 Business Analysis. Regardless of which tool/method is used, an understanding of the following, at a minimum, must be clearly articulated:

- Functional requirements
- Expected user experience(s)
- Expected system outcome

- Expected business operations (e.g., How do you envision operations in the future?)
- Alignment to the project's objectives identified in Stage 1
- Product ownership (e.g., Who owns these requirements?); and
- Verification of need(s) fulfillment (e.g., How will success be measured?)

Tip: If providing requirements, the recommended range of requirements is between 50 and 100.

Attach Requirements and/or Outcomes narratives, mid-level requirements, and/or epics/user stories to submission email.

Requirements have been attached as:

2.04.0 Midlevel_Solution_Requirements.xlxm

2.5 Assumptions and Constraints

Relevant assumptions and constraints help define boundaries and opportunities to shape the scope and complexity of the project.

Assumption: OIG-HSR staff will continue to use Authority-provided IT hardware (laptops, phones) to access the new system.

> **Description/Potential Impact**: Software procured is subject to Authority-provided hardware technical specifications and security
>
> **Description/Potential Impact**: Authority-provided hardware becomes unavailable or restricted, or if auxiliary equipment needs to be procured, increasing project costs and delaying implementation. However, state law requires the Authority to provide needed IT services and equipment to the OIG-HSR and tis staff, making this impact extremely unlikely.

Assumption: Vendors under consideration must offer FedRAMP-compliant hosting environments that meet State of California information security requirements.

> **Description/Potential Impact**: OIG-HSR is only considering FedRAMP-compliant vendors

Assumption: FY 2025–26 implementation funding will be approved as part of the budget process.

> **Description/Potential Impact**: Without approved funding, project execution cannot proceed. However, project costs for FY2025-26 are included in an approved budget change proposal from OIG-HSR that is currently included in the Legislature's approved budget.

Assumption: Authority IT will allow secure and limited system access (e.g., network routing, endpoint access) without having data-level visibility.

> **Description/Potential Impact**: As noted above, the Authority is legally required to provide network access to OIG-HSR, but any challenges in establishing this arrangement could result in delays. For this very reason, OIG-HSR has listed the Authority as a project stakeholder, and OIG-HSR management has been in communication with Authority IT executives at the Authority to plan for implementing the eventual project on its network.

Assumption: OIG-HSR can administer the selected solution without needing to establish a full internal IT function.

> **Description/Potential Impact**: If vendor or system limitations require significant in-house technical support, it may necessitate staffing or procurement changes, increasing project complexity. However, the widely used nature of the Saas products under consideration by state and federal inspectors general and auditors make unwieldy technical support requirements unlikely.

Assumption: The user base (internal and external) will require minimal training due to the vendor's intuitive design and provided support materials.

> **Description/Potential Impact**: If training needs are underestimated, it could delay rollout and decrease early adoption or accurate data entry. However, the widely used nature of the Saas products under consideration by state and federal inspectors general and auditors make it unlikely that the need for training would be extensive enough to cause delays in implementation. Further, OIG-HSR's relatively small group of ultimate users makes training more efficient to roll out and reinforce on a small group or one-to-one basis as needed.

Assumption: No major legislative or regulatory changes related to confidentiality or case management will occur during project implementation.

> **Description/Potential Impact**: New legislation or regulations could require rework or system changes, impacting cost and timeline.

Constraint: The system must be fully operational before the end of FY 2025–26

> **Description/Potential Impact**: Delays may result in failure to meet strategic objectives and further delay OIG-HSR's ability to demonstrate full compliance with statutory mandates for confidentiality.

TIP: Copy and paste to add Assumptions/Constraints with Descriptions/Impacts as needed.

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.

Dependency Element: Authority Network Access

> **Dependency Description**: OIG-HSR requires continued ability to use Authority-provided hardware and internet to connect to the new system.

Dependency Element: FY 2025–26 Budget Approval

Dependency Description: Project execution is contingent on funding approval through the FY 2025–26 Budget Change Proposal submitted in August 2024.

Dependency Element: Vendor FedRAMP Certification

Dependency Description: The selected vendor must maintain active FedRAMP certification for hosting data in compliance with federal and state security requirements.

Dependency Element: Timely Procurement Execution

Dependency Description: Project relies on successful completion of competitive procurement activities and contract execution before the end of fiscal year 2025-2026

Dependency Element: Security & Privacy Compliance Reviews

Dependency Description: Approval of a Privacy Threshold Assessment (PTA), as well as compliance with state security policies and applicable IT policies, is required for go-live.

TIP: Copy and paste to add Dependency Elements and Descriptions as needed.

2.7 Market Research

Market Research (CDT Market Research Guidelines) determines whether products or services available in the marketplace can meet the business needs identified in this proposal. Market Research can also determine whether commercial practices regarding customizing/modifying products or tailoring services are available, or even necessary, to meet the business needs and objectives of the business.

Before undertaking a Market Research approach. Contact your PAO Manager to schedule a collaborative review to review planning to date and discuss the procurement approach.

1. **Project Management Methodology:** Adaptive Approach (Agile)
2. **Procurement approach recommended:** Standard Procurement
3. **Market Research Approach**

   Provide a concise narrative description of the approach used to perform market research.

   The OIG-HSR conducted extensive market research to evaluate commercially available audit management software solutions capable of replacing current manual processes and supporting the office's statutory mandate to conduct independent audits, and to do so in a way that better ensures accuracy and compliance with relevant professional standards. This research aimed to identify a product that meets information security standards, enables efficient audit workflows, and aligns with public sector audit requirements such as GAGAS.

   Four products were reviewed in depth: AuditBoard, Workiva, Diligent, and TeamMate+. Evaluation criteria included FedRAMP or equivalent information security compliance, audit workflow functionality (planning, execution, and follow-up), document control, simultaneous collaboration, access control, reporting, pricing, and existing state agency adoption.

- AuditBoard is cloud-based platform offering templates, dashboards, and automated reminders. However, it lacks FedRAMP certification, which may disqualify it for state use.
- Workiva has robust internal audit features, FedRAMP certification, a collaborative interface with no document check-in/check-out required, and built-in risk analytics. Workiva is used by major government and corporate clients and provides over 3,000 audit-related templates.
- Diligent supports both audits and investigations and is FedRAMP certified and includes advanced reporting, corrective action workflows, and integration with whistleblower portals. However, some limitations were noted in document linking and Microsoft Word compatibility.
- TeamMate+ is in use by over 20 California departments and offers FedRAMP-compliant hosting, configurable audit workflows, integrated time tracking, analytics, and extensive report templates. Other features include issue tracking, simultaneous user notifications, and alignment with audit standards.

Among evaluated solutions, Workiva best satisfied mandatory and desirable criteria, including FedRAMP compliance, access controls, large document handling, robust audit trails, coaching notes, templates, and budget tracking. This research was supported by demo requests, peer feedback , and review of supplier purchase histories across the State. The information gathered will inform the alternatives analysis and eventual procurement decision in Stage 3.

4. **Market Research Artifacts**

   Market Research Artifacts can include internet research, collaboration with other governmental entities, or other documentation.

   Attach Market Research artifacts to the email submission.

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 should provide at minimum the three (3) most viable solutions, one (1) of which could be leveraging and/or enhancing the existing solution (if applicable).

1. **Viable Alternative Solution #1**

   Name: Procurement of SaaS Audit Management System

   Description: Acquire a cloud-based, audit-specific software solution like Workiva, Opexus, or Diligent, all of which were evaluated through market research. These platforms support documentation, review workflows, role-based access, and tracking/reporting required under professional audit standards.

   Why is this a viable solution? Please explain:

   This is the only alternative that meets all statutory, professional, and technical requirements. SaaS options offer faster deployment, scalability, and built-in compliance features (e.g., version control,

audit trails, templates). Workiva offers the strongest combination of performance, usability, and support for simultaneous editing.

Approach

Increase staff – new or existing capabilities: No

Modify the existing business process or create a new business process: Yes

Reduce the services or level of services provided: No

Utilize new or increased contracted services: Yes

Enhance the existing IT system: No

Modify Statute/Policy/Regulations: No

Please Specify: Click or tap here to enter text.

Create a new IT system: No

Other: No Specify: Click or tap here to enter text.

Architecture Information

Business Function(s)/Process(es): Risk Assessment, Audit Lifecycle, Recommendations

TIP: Copy and paste or click the + button in the lower right corner 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.

Conceptual Architecture

Attach a copy of the conceptual architecture to your email submission.

COTS/SaaS/Cloud Technology or Custom: COTS/SaaS/Cloud Technology

Name/Primary Technology: Workiva

TIP: Copy and paste or click the + button in the lower right corner to add system software information if the application, system, or component uses additional system software.

Explain Existing System Interfaces: N/A

Explain New System Interfaces: N/A

Data Center Location of the To-be Solution: Agency/state entity operated by agency/state entity

If Other, specify: Click or tap here to enter text.

Security

Access

Public: Yes

Internal State Staff: Yes

External State Staff: No

Other: No Specify: Click or tap here to enter text.

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: Yes

Health: No

Tax: No

Financial: No

Legal: Yes

Confidential: Yes

Other: No Specify: Click or tap here to enter text.

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

Technical Security: Yes

Physical Security: Yes

Backup and Recovery: Yes

Identity Authorization and Authentication: Yes

Other, specify: Click or tap here to enter text.

Total Viable Alternative #1 Solution Cost (copy from FAW – Executive Cost Summary tab, cells E7 through E11):

Planning Costs: $437,294

One-Time (Project) Costs: $442,724

Total Future Ops. IT Staff OE&E Costs: $235,000

Total Proposed Cost: $1,175,018

Annual Future Ops. Costs (M&O): $100,000

2. **Viable Alternative Solution #2**

Name: Custom Development of an Audit Management System

Description: Develop a custom-built audit management platform using contracted IT staff or vendor developers. The system would be tailored to OIG-HSR's standards and processes but built from the ground up.

Why is this a viable solution? Please explain:

Custom development allows for maximum control and flexibility in design. It can be tailored to meet every audit process requirement, including integration with internal policies and document flow. However, this option requires significant budget, time, and testing to meet security and auditability standards.

Approach

Increase staff – new or existing capabilities: No

Modify the existing business process or create a new business process: Yes

Reduce the services or level of services provided: No

Utilize new or increased contracted services: Yes

Enhance the existing IT system: No

Modify Statute/Policy/Regulations: No

Please Specify: Click or tap here to enter text.

Create a new IT system: Yes

Other: No Specify: Click or tap here to enter text.

Architecture Information

Business Function(s)/Process(es): Risk Assessment, Audit Lifecycle, Recommendations

TIP: Copy and paste or click the + button in the lower right corner 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.

Conceptual Architecture

Attach a copy of the conceptual architecture to your email submission.

COTS/SaaS/Cloud Technology or Custom: Custom

Name/Primary Technology: Custom Development

TIP: Copy and paste or click the + button in the lower right corner to add system software information if the application, system, or component uses additional system software.

Explain Existing System Interfaces: N/A

Explain New System Interfaces: N/A

Data Center Location of the To-be Solution: Agency/state entity operated by agency/state entity

If Other, specify: Click or tap here to enter text.

Security

Access:

Public: Yes

Internal State Staff: Yes

External State Staff: No

Other: No Specify: Click or tap here to enter text.

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: Yes

Health: No

Tax: No

Financial: No

Legal: Yes

Confidential: Yes

Other: No Specify: Click or tap here to enter text.

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

Technical Security: Yes

Physical Security: Yes

Backup and Recovery: Yes

Identity Authorization and Authentication: Yes

Other, specify: Click or tap here to enter text.

Total Viable Alternative #2 Solution Cost (copy from FAW – Summary tab, cell AL33):

Total Proposed Cost: $4,000,867

3. **Viable Alternative Solution #3**

Name: Continue Current Manual Workflow (Word/Excel)

Description: Continue using Microsoft Word, Excel, and shared drives for audit documentation, review notes, and recommendations tracking.

Why is this a viable solution? Please explain:

This alternative involves no new costs or procurement. However, it creates significant challenges to OIG efforts to implement professional audit standards and document audit workflows efficiently, and lacks security, audit trails, and automated reporting. It is unsustainable as audit volume and

complexity increase, introducing unnecessary risk to the OIG-HSR and oversight of the high-speed rail project itself.

Approach

Increase staff – new or existing capabilities: No

Modify the existing business process or create a new business process: No

Reduce the services or level of services provided: Choose Yes or No.

Utilize new or increased contracted services: Yes

Enhance the existing IT system: No

Modify Statute/Policy/Regulations: No

Please Specify: Click or tap here to enter text.

Create a new IT system: No

Other: Choose Yes or No. Specify: Click or tap here to enter text.

Architecture Information

Business Function(s)/Process(es): Risk Assessment, Audit Lifecycle, Recommendations

TIP: Copy and paste or click the + button in the lower right corner 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.

Conceptual Architecture

Attach a copy of the conceptual architecture to your email submission.

COTS/SaaS/Cloud Technology or Custom: Custom

Name/Primary Technology: Email and Phone

TIP: Copy and paste or click the + button in the lower right corner to add system software information if the application, system, or component uses additional system software.

Explain Existing System Interfaces: No System Interfaces

Explain New System Interfaces: No New System Interfaces

Data Center Location of the To-be Solution: Agency/state entity operated by agency/state entity

If Other, specify: Click or tap here to enter text.

Security

Access:

Public: Yes

Internal State Staff: Yes

External State Staff: No

Other: No Specify: Click or tap here to enter text.

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: Yes

Health: No

Tax: No

Financial: No

Legal: Yes

Confidential: Yes

Other: No Specify: Click or tap here to enter text.

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

Technical Security: Yes

Physical Security: Yes

Backup and Recovery: Yes

Identity Authorization and Authentication: Yes

Other, specify: Click or tap here to enter text.

Total Viable Alternative #3 Solution Cost (copy from FAW – Summary tab, cell AL50):

Total Proposed Cost: $421,294

2.9 Project Organization

Project planning includes the process of identifying how and when specific labor skill sets are needed to ensure that the proposed project has sufficient staff with the appropriate knowledge and experience by the time the project moves into execution. All staff identified in the following sections should be included in the Financial Analysis Worksheet to be completed in Section 2.12.

1. **Project Organization Chart:**

   Attach the Project Organization Chart to your email submission.

2. **Is the department running this project as a matrixed or projectized organization?**

   Projectized

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.

1. **Administrative**

   Administrative functions will be supported by OIG staff. This includes logistical coordination, document management, meeting facilitation, and maintaining project documentation and records. OIG staff will ensure these functions are performed in parallel with ongoing operations to minimize disruption to core responsibilities.

2. **Business Program**

   OIG staff will serve as end users and as subject matter experts contributing business knowledge throughout the project, particularly during requirements definition, design validation, and functional testing and User Acceptance Testing. While temporary deferral of lower-priority activities may be used to manage workload during product installation, the procurement of an industry standard SaaS application should minimize the amount of support needed during implementation.

3. **Information Technology**

   General IT infrastructure support will continue to be provided by the Authority, while the vendor will be responsible for configuring, operating, and maintaining the system. Because the system is externally hosted, no additional burden is expected on internal IT staff. OIG staff will coordinate with the vendor for secure access, user provisioning, and ongoing support as needed.

4. **Testing**

   System testing responsibilities will be shared between the vendor and OIG. The vendor will conduct system integration testing and technical testing, while OIG staff will be responsible for developing user acceptance test scripts, coordinating test sessions, and validating that the system meets business needs.

5. **Data Conversion/Migration**

   Data conversion is not applicable for this project, as the existing process is manual and no legacy case data will be migrated into the new system.

6. **Training**

   The vendor will provide video-based training and/or live virtual training sessions tailored to OIG roles. This training approach will minimize impact to OIG resources and allow for self-paced learning and adoption.

7. Organizational Change Management

OCM activities related to the project will include project announcements and communications to end users. OIG will apply change management strategies throughout implementation. These include early stakeholder involvement, regular project updates, training tailored to specific roles, and active communication to ensure business readiness and promote user adoption of the new system.

8. Resource Capacity/Skills/Knowledge for Stage 3 Solution Development

This narrative should include the experience level and quantity of procurement, contract management, and budget staff who will be responsible for the Stage 3 Solution Development.

Stage 3 will be supported by the same OIG team that led Stage 2. This team includes experienced staff in procurement, contract oversight, and budget planning. Their direct involvement in developing the Stage 2 alternatives and conducting market research ensures continuity and preparedness as the project transitions to solution development, solicitation, and vendor selection.

2.10 Project Planning

1. Project Management Risk Assessment

Updated Project Management Risk Score: 1.1

Attach Updated PM Risk Assessment to your email submission. SIMM Section 45A

2. Project Charter

Is your project charter approved by the designated Agency/state entity authority and available for the Department of Technology to review? **Choose**: 'Yes,' 'No,' or 'Not Applicable.' If 'No' or 'Not Applicable,' provide the artifact status in the space provided.

Project Charter (Approved): Yes

Status: Click or tap here to enter text.

Attach a copy of the Project Charter to your email submission.

3. Project Plans

Are the following project management plans or project artifacts approved by the designated Agency/state entity authority and available for the Department of Technology to review? **Choose**: 'Yes,' 'No,' or 'Not Applicable.' If 'No' or 'Not Applicable,' provide the artifact status in the space provided.

Note: For Low to medium complexity and cost projects, discuss with your PAO manager the option of submitting a Master Project Management Plan in place of individual plans.

Scope Management Plan (Approved): Yes

Status: Click or tap here to enter text.

Communication Management Plan (Approved): Yes

Status: Click or tap here to enter text.

Schedule Management Plan (Approved) : Yes

Status: Click or tap here to enter text.

Procurement Management Plan (Approved): Yes

Status: Click or tap here to enter text.

Requirements Management Plan (Approved): Yes

Status: Click or tap here to enter text.

Stakeholder Management Plan (Draft): Yes

Status: Click or tap here to enter text.

Governance Plan (Draft): Yes

Status: Click or tap here to enter text.

Contract Management Plan (Draft): Yes

Status: Click or tap here to enter text.

Resource Management Plan (Draft): Yes

Status: Click or tap here to enter text.

Change Control Management Plan (Draft): Yes

Status: Click or tap here to enter text.

Risk Management Plan (Draft + Risk Log): Yes

Status: Click or tap here to enter text.

Issue and Action Item Management Plan (Draft + Issue Log): Yes

Status: Click or tap here to enter text.

Cost Management Plan (Approved if planning BCP approved): Yes

Status: Click or tap here to enter text.

4. **Project Roadmap (High-Level)**

   Attach a high-level Project Roadmap showing remainder of planning phase and transition into execution phase to the email submission.

   a) Planning Start Date: 8/1/2024

   b) Estimated Planning End Date: 6/30/2026

   c) Estimated Project Start Date: 7/1/2026

   d) Estimated Project End Date: 6/30/2028

2.11 Data Cleansing, Conversion, and Migration

If in Section 2.3 (above) the answer to the question "Do you have existing data that must be migrated to your new solution?" was marked "Yes," please complete this section.

The California Department of Technology recommends having a Data Consultant start data cleansing, conversion, and migration activities as soon as possible.

Identify the status of each of the following data activities. If "Not Applicable" is chosen, explain why the activity is not applicable or if "Not Started" is chosen, explain when the activity will start and its anticipated duration:

1. **Current Environment Analysis: Not Applicable**

   Click or tap here to enter text.

2. **Data Migration Plan: Not Applicable**

   Click or tap here to enter text.

3. **Data Profiling: Not Applicable**

   Click or tap here to enter text.

4. **Data Cleansing and Correction: Not Applicable**

   Click or tap here to enter text.

5. **Data Quality Assessment: Not Applicable**

   Click or tap here to enter text.

6. **Data Quality Business Rules: Not Applicable**

   Click or tap here to enter text.

7. **Data Dictionaries: Not Applicable**

   Click or tap here to enter text.

8. **Data Conversion/Migration Requirements: Not Applicable**

   Click or tap here to enter text.

2.12 Financial Analysis Worksheets

Attach F.2 Financial Analysis Worksheet(s) to the email submission.

End of agency/state entity document.

Please ensure ADA compliance before submitting this document to CDT.

When ready, submit Stage 2 and all attachments in an email to ProjectOversight@state.ca.gov.

Department of Technology Use Only

Original "New Submission" Date: 7/1/2025 **Form**

Received Date: 7/1/2025

Form Accepted Date: 7/1/2025

Form Status: In Analysis

Form Status Date: 7/1/2025

Form Disposition: Approved

Form Disposition Date: 08/26/2025.