



Stage 1 Business Analysis

California Department of Technology, SIMM 19A.2 (Rev. 2.4), Revised 4/2/2018

1.1 General Information

Agency or State Entity Name:	California Department of Technology
Organization Code:	
Proposal Name:	Unified Integrated Risk Management (UIRM)
Proposal Description:	For California state government information security programs to successfully improve against a backdrop of ever increasing and sophisticated threats, we must be able to effectively manage security risks and measure maturity across the enterprise and within each state entity. Doing so requires automation of reporting, security compliance, program and policy management, asset management, incident management, oversight, audits, assessment tracking and reporting.
When do you want to start this project?:	01/04/2021
Department of Technology Project Number:	7502-006

1.2 Submittal Information

Contact Information:	
Contact First Name	Contact Last Name
Kathy	Cruz
Contact Email	Contact Phone Number
Kathy.Cruz@state.ca.gov	916-431-5542
Submission Date:	1/14/2019
Version Number:	1.0 Paper
Project Approval Executive Transmittal	
Attachment: Include the Project Approval Executive Transmittal as an attachment to your email submission.	

1.3 Business Sponsorship

Executive Sponsors			
Title	First Name	Last Name	Business Program Area
State Chief Information Security Officer	Peter	Liebert	Office of Information Security
Select + to add additional Executive Sponsors			
Business Owners			
Title	First Name	Last Name	Business Program Area
Manager	Michael	Stanford	OIS Audits
Manager	Helen	Woodman	OIS Audits, Assessments and Advisory Services



Stage 1 Business Analysis

California Department of Technology, SIMM 19A.2 (Rev. 2.4), Revised 4/2/2018

Manager	Michele	Robinson	OIS Security Risk Governance
AISO GovOps/BCHSA	Nadean	Shavor	Agency Information Security Officer
AISO CHSA	Christine	Schmoeckel	Agency Information Security Officer
AISO CNRA	Glen	Carson	Agency Information Security Officer
AISO DOF	Brently	Foon	Agency Information Security Officer
AISO CalVet	Ernest	Shih	Agency Information Security Officer
AISO CalEPA	Mike	Marshall	Agency Information Security Officer
AISO CalSTA	Karl	Kopper	Agency Information Security Officer

Select + to add additional Business Owners

Program Background and Context

Government Code 11549-11549.4

11549 (a) The purpose of the Office of Information Security is to ensure the confidentiality, integrity and availability of state systems and applications, to promote and protect privacy as part of the development and operations of state systems and applications to ensure the trust of the residents of this state. 11549 (c) The duties of the Office of Information Security, under the direction of the chief, shall be to provide direction for information security and privacy



Stage 1 Business Analysis

California Department of Technology, SIMM 19A.2 (Rev. 2.4), Revised 4/2/2018

to state government agencies, departments and offices. 11549.3 (a) The chief shall establish an information security program.

1.4 Stakeholders

Key Stakeholders

Org. Name	Name		
All State Entities	OIS, AISOs, ISOs		
Internal or External?	<input checked="" type="checkbox"/> Internal <input checked="" type="checkbox"/> External		
When is the Stakeholder Impacted?			
Input to Business Process	During the Business Process	Output of the Business Process	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

How are Stakeholders impacted?

3000

How will the Stakeholders participate in the project?

Project governance using project management best practices will be implemented.

The ISOs (stakeholders) will receive regular project updates and will participate in functional requirements development workshops and teams.

System users will participate in functional requirements development workshops and teams.

The business owners (OIS managers and AISOs) will receive a project report weekly, be briefed at minimum monthly and will participate in all major project decisions. Additionally, the business owners will actively participate in functional requirement development workshops and teams.

Select + to add additional Stakeholders

1.5 Business Program

Org. Name	Name		
All Information Security Programs are impacted			
When is the unit Impacted?			
Input to the Business Process	During the Business Process	Output of the Business Process	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

How is the business program unit impacted?

How will the business program participate in the project?

Select + to add additional Business Programs

1.6 Business Alignment

Business Driver(s)

Financial Benefit

Increased Revenue	Cost Savings	Cost Avoidance	Cost Recovery
-------------------	--------------	----------------	---------------



Stage 1 Business Analysis

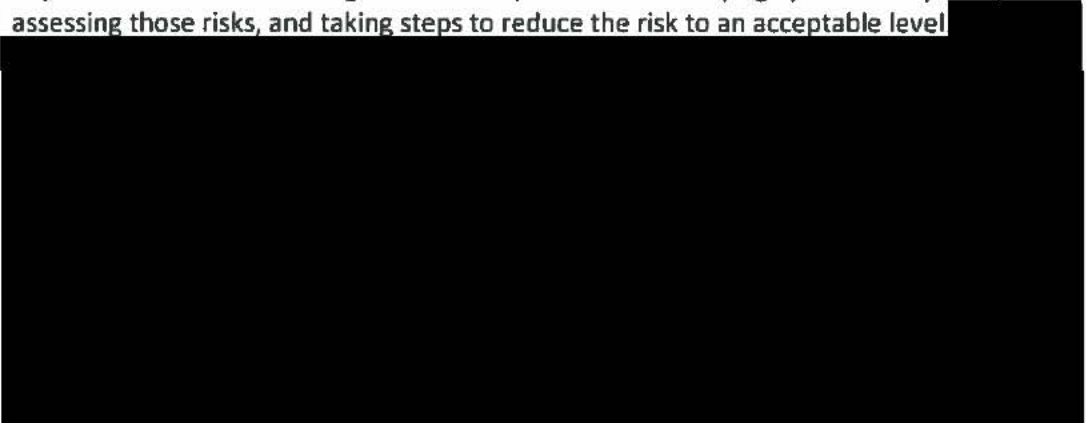
California Department of Technology, SIMM 19A.2 (Rev. 2.4), Revised 4/2/2018

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Mandate(s)			
State		Federal	
<input type="checkbox"/>		<input type="checkbox"/>	
Improvement			
Better Services to Citizens	Efficiencies to Program Operations	Improved Health and/or Human Safety	Technology Refresh
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Security			
Improved Information Security	Improved Business Continuity	Improved Technology Recovery	Technology End of Life
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Strategic Business Alignment			
Strategic Plan Last Updated?		11/1/2017	
Strategic Business Goal		Alignment	
Advance the maturity of information security across California government.		This proposal directly aligns by provided fundamental functionality to increase maturity in all state entities in being able to quickly and effectively document, monitor and escalate information security issues.	
<i>Select + to add additional Business Goals and Alignment</i>			
Executive Summary of the Business Problem or Opportunity			
Business Problem or Opportunity and Objectives Table			
Problem ID	Problems/Opportunities		
	[Redacted Content]		
Objective ID	1.1		
Objectives	Implement an Integrated Risk Management (IRM) platform with security incident lifecycle management capabilities. Transition users and data from the current Cal-CSIRS incident reporting system to the IRM platform. For state entities with Security Information and Event Management (SIEM) capabilities, complete integration of SIEMS		



Stage 1 Business Analysis

California Department of Technology, SIMM 19A.2 (Rev. 2.4), Revised 4/2/2018

	into the incident management module. Enable notification management, alerts and triggers. Objective is 100% adoption during the first year of implementation.
Metric	All state entities and OIS on one platform for incident management
Baseline	
Target	100%
Measurement Method	
<i>Select + to add additional Objectives</i>	
<i>Select + to add additional Problems</i>	
Problem ID	Problems/Opportunities
2 Risk Management	<p>In the face of ever increasing cyber threats, including advanced malware, well-funded and organized adversaries and automated cybersecurity attacks, the State must prioritize its resources to manage the most significant risk to its services and the populations that depend on them. Risk management is the process of identifying cybersecurity risks, assessing those risks, and taking steps to reduce the risk to an acceptable level</p> 
Objective ID	2.1
Objectives	Implement an Integrated Risk Management (IRM) platform with the full suite of risk management functionality required by both OIS and state entities. All state entities and OIS are managing information security risks using the platform tools. Plans of Actions and Milestones (POAMs), risk assessments, risk registers, risk variants, risk profiles, risk scores and risk alerts are through a single IRM workflow and platform. All data from existing POAMs have been uploaded and any relevant data from existing GRC tools have been uploaded.
Metric	All risk management activities on a single platform
Baseline	
Target	
Measurement Method	
<i>Select + to add additional Objectives</i>	

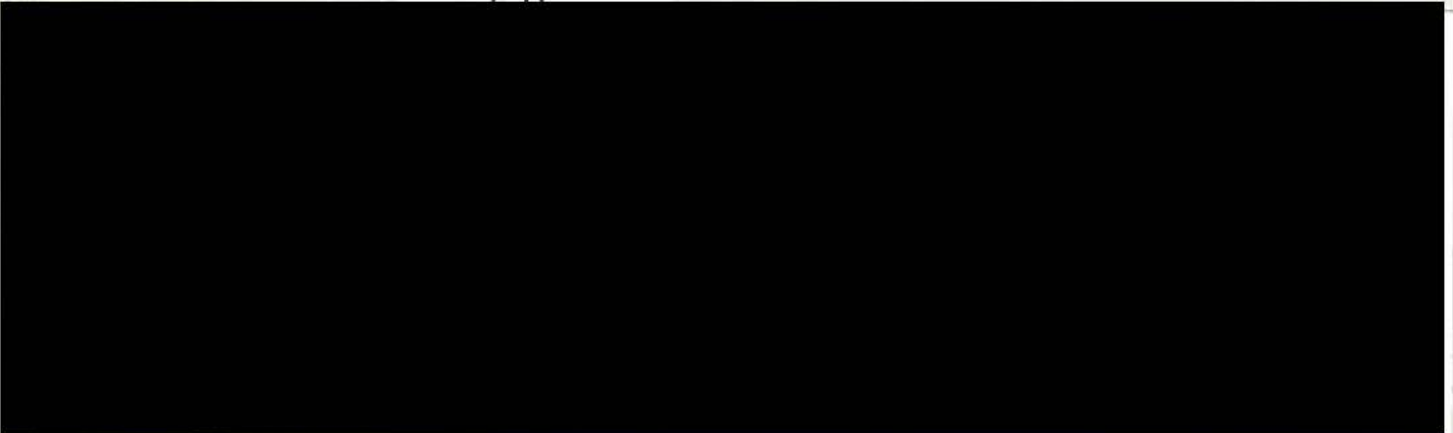


Stage 1 Business Analysis

California Department of Technology, SIMM 19A.2 (Rev. 2.4), Revised 4/2/2018

Problem ID

Problems/Opportunities



Objective ID

3.1

Objectives

OIS audits and assessments are conducted and completed using a single IRM platform. OIS is able to conduct continuous reviews of changes and additions to artifacts, eliminating the need for audited state entities to transmit 150 individual artifacts electronically for each audit. Maturity metrics gathered during audits and independent assessments are integrated into the IRM platform allowing for continuous updating of maturity metrics and risk profiles. Engagement scheduling, notifications and tracking is automated and work papers, audit findings and reports are in a single secure repository. Draft and final audit reports are automated.

Metric

All audits and assessment activities, documents and notifications are on a single platform

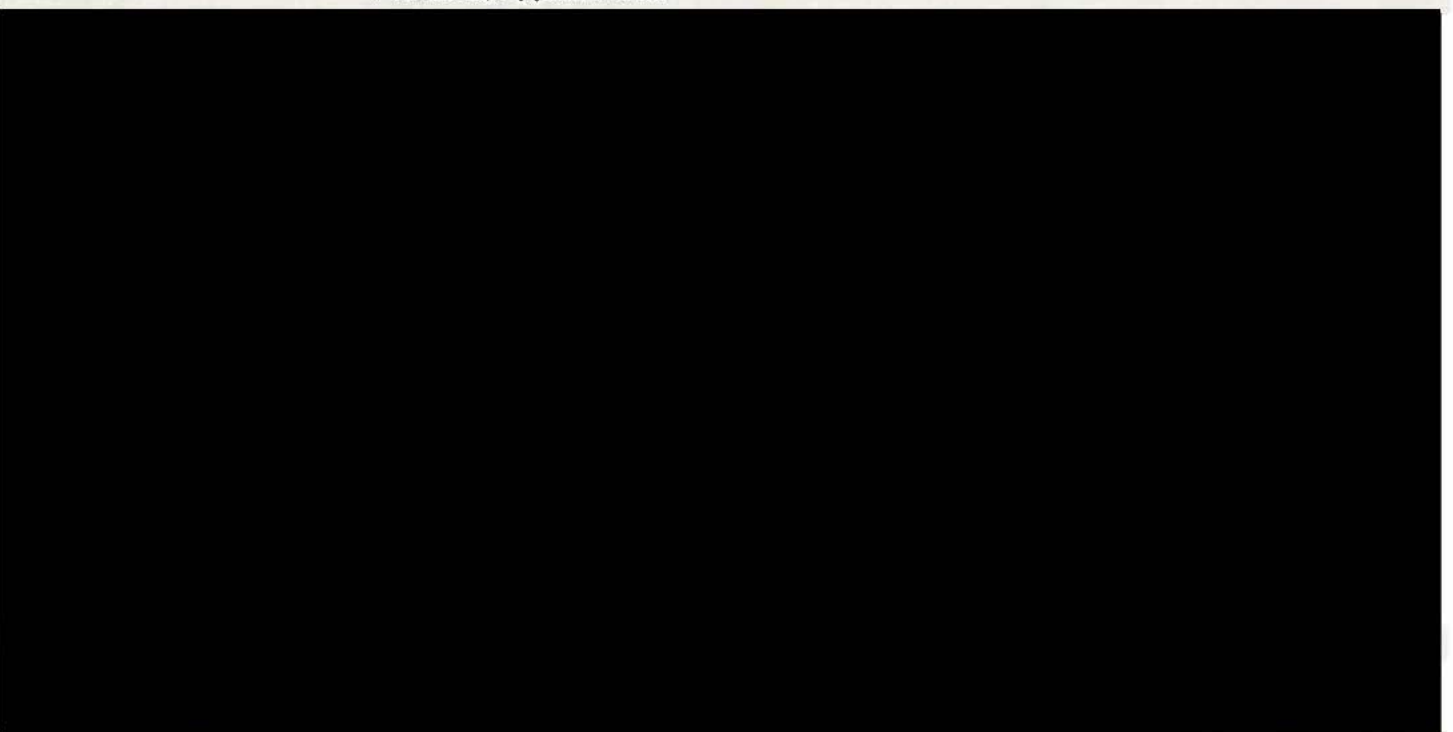
Baseline

Target

Measurement Method

Problem ID

Problems/Opportunities





Stage 1 Business Analysis

California Department of Technology, SIMM 19A.2 (Rev. 2.4), Revised 4/2/2018

management, variances, acknowledgement, mapping, version control, review and communications are performed using a single IRM platform. All OIS compliance and oversight review of submissions by state entities such as Plan of Action and Milestones (POAM), Technology Recovery Plans (TRP), Privacy program reviews, Designation Letters, notifications and tracking will be accomplished through the IRM platform. Agencies and state entities will no longer need to email, hand-deliver or submit through secure file transfer compliance documents required in SAM 5300 and SIMM 5300. Rather, OIS will be able to review, comment and request via the IRM platform.

Metric	All audits and assessment activities, documents and notifications are on a single platform
Baseline	
Target	
Measurement Method	

Problem ID Problems/Opportunities



Objective ID

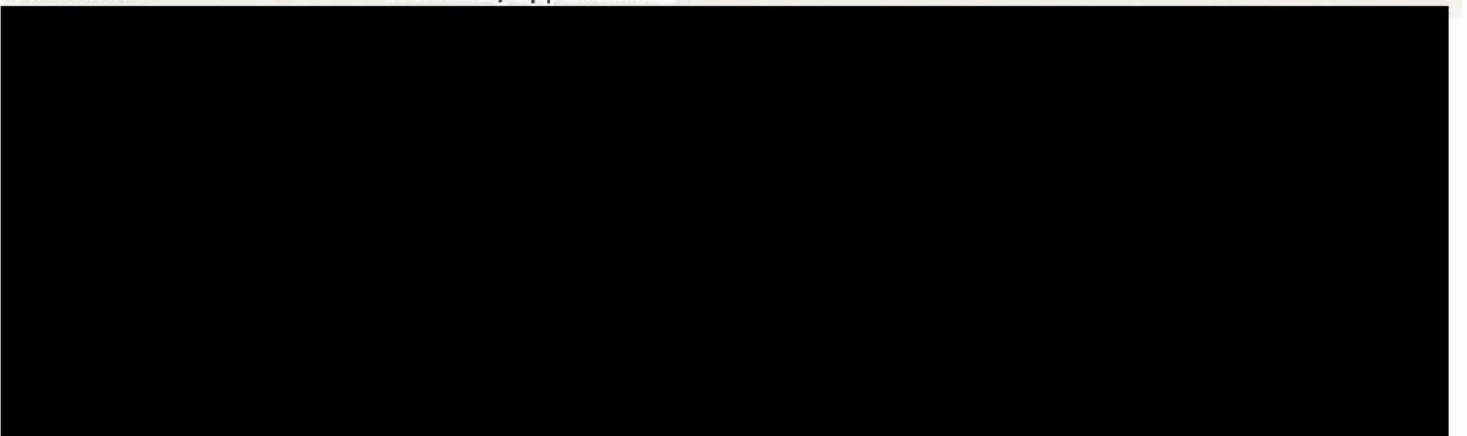
5,1 State entities have all IT assets in a single repository, can map assets to identified risks and can populate this information into the risk management module and POAM as appropriate. Threat alerts related to specific assets can be quickly identified and notifications sent of needed actions. Tracking of remediation and/or removal can also be tracked.

Metric

All IT asset inventories on a single platform

Target

Problem ID Problems/Opportunities



Objective ID



Stage 1 Business Analysis

California Department of Technology, SIMM 19A.2 (Rev. 2.4), Revised 4/2/2018

- 6.1 Multi-tiered dashboard for state entities, Agency, leadership reporting and OIS are enabled. Triggered notifications are enabled alerting state entities and/or Agencies of reporting, and compliance requirements and dates. OIS has multi-view and easily customizable dashboards of enterprise risk, compliance and governance with drill-down on clusters and variables. Real-time information for reporting and decision-making is continuously available.

Metric

Automated reporting, metrics, dashboards, triggers, notificaitons and alerts

Target

Project Approval Lifecycle Completion and Project Execution Capacity Assessment

1. Does the proposal development or project execution anticipate sharing resources (state staff, vendors, consultants or financial) with other priorities within the Agency/state entity (projects, PALs, or programmatic/technology workload)?

☒ Yes ☐ No ☐ Clear

2. Does the Agency/ state entity anticipate this proposal will result in the creation of new business processes or changes to existing business processes?

☐ No ☐ New Processes ☐ Existing Processes ☒ Both New and Existing ☐ Clear

1.7 Project Management

Project Management Risk Score:

Attach completed Statewide Information Management Manual (SIMM) Section 45 Appendix A:

Include the completed SIMM 45 Appendix A as an attachment to your email submission.

Existing Data Governance and Data

1. Does the Agency/state entity have an established data governance body with well-defined roles and responsibilities to support data governance activities? If an existing data governance org chart is used, please attach.

☐ Unknown
☒ Yes
☐ No
☐ Clear

If applicable, include the data governance org chart as an attachment to your email submission.

2. Does the Agency/state entity have data governance policies (data policies, data standards, etc.) formally defined, documented, and implemented? If yes, please attach the existing data governance plan, policies or IT standards used.

☐ Unknown
☒ Yes
☐ No
☐ Clear

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

3. Does the Agency/state entity have data security policies, standards, controls, and procedures formally defined, documented, and implemented? If yes, please attach the existing documented security policies, standards, and controls used.

☐ Unknown
☒ Yes
☐ No
☐ Clear

If applicable, include the documented security policies, standards, and controls as an attachment to your email submission.



Stage 1 Business Analysis

California Department of Technology, SIMM 19A.2 (Rev. 2.4), Revised 4/2/2018

4. Does the Agency/state entity have user accessibility policies, standards, controls, and procedures formally defined, documented, and implemented? If yes, please attach the existing documented policies, accessibility governance plan, and standards used, or provide additional information below.	<input type="radio"/> Unknown <input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Clear	If applicable, include the documented accessibility policies, standards, and controls as an attachment to your email submission.
5. Do you have existing data that you are going to want to access in your new solution?	<input type="radio"/> Unknown <input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Clear	If applicable, include the data migration plan as an attachment to your email submission.
6. If data migration is required, please rate the quality of the data.	Select...	

1.8 Criticality Assessment

Business Criticality

Legislative Mandates:	N/A <input checked="" type="checkbox"/>	
Bill Number(s)/Code(s):		
Language that includes system relevant requirements:		
Business Complexity Score	2.2	Include the completed SIMM 45 Appendix C as an attachment to your email submission.

Noncompliance Issues

Indicate if your current operations include noncompliance issues and provide a narrative explaining the how the business process is noncompliant.

Programmatic Regulations	HIPPA/CJIS/FTI/PII/PCI	Security	ADA	Other	N/A
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

1. What is the proposed project start date?	1/1/2021		
2. Is this proposal anticipated to have high public visibility?	<input type="radio"/> Yes <input checked="" type="radio"/> No <input type="radio"/> Clear		
If "Yes," please identify the dynamics of the anticipated high visibility below:			
3. If there is an existing Privacy Information Assessment, include as an attachment to your email submission.			
4. Does this proposal affect business program staff located in multiple geographic locations?	<input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Clear		
If "Yes," provide an overview of the geographic dynamics below and enter the specific information in the space provided.			
This solution will be used by every state entity within the state.			
City	State	Number of Locations	Approximate Number of Staff
Select + to add Locations			

1.9 Funding



Stage 1 Business Analysis

California Department of Technology, SIMM 19A.2 (Rev. 2.4), Revised 4/2/2018

1. Does the Agency/state entity anticipate requesting additional resources through a budget action to complete the project approval lifecycle?		<input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Clear
2. Will the state possibly incur a financial sanction or penalty if this proposal is not implemented? If yes, please identify the financial impact to the state below:		<input type="radio"/> Yes <input checked="" type="radio"/> No <input type="radio"/> Clear
3. Has the funding source(s) been identified for this proposal?		<input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Clear
FUNDING SOURCE		FUND AVAILABILITY DATE
General Fund	<input checked="" type="checkbox"/>	7/1/2020
Special Fund	<input type="checkbox"/>	Date Picker
Federal Fund	<input type="checkbox"/>	Date Picker
Reimbursement	<input type="checkbox"/>	Date Picker
Bond Fund	<input type="checkbox"/>	Date Picker
Other Fund	<input type="checkbox"/>	Date Picker
If "Other Fund" is checked, specify the funding:		
1.10 Reportability Assessment		
1. Does the Agency/state entity's IT activity meet the definition of an IT Project found in the State administrative Manual (SAM) Section 4819.2? If "No," this initiative is not an IT project and is not required to complete the Project Approval Lifecycle.		<input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Clear
2. Does the activity meet the definition of Maintenance or Operations found in SAM Section 4819.2? If "Yes," this initiative is not required to complete the Project Approval Lifecycle. Please report this workload on the Agency Portfolio Report. And provide an explanation below.		<input type="radio"/> Yes <input checked="" type="radio"/> No <input type="radio"/> Clear
3. Has the project/effort been previously approved and considered an ongoing IT activity identified in SAM Section 4819.2, 4819.40? If "Yes," this initiative is not required to complete the Project Approval Lifecycle. Please report this workload on the Agency Portfolio Report.		<input type="radio"/> Yes <input checked="" type="radio"/> No <input type="radio"/> Clear



Stage 1 Business Analysis

California Department of Technology, SIMM 19A.2 (Rev. 2.4), Revised 4/2/2018

4. Is the project directly associated with any of the following as defined by SAM Section 4812.32? Single-function process-control systems; analog data collection devices, or telemetry systems; telecommunications equipment used exclusively for voice communications; Voice Over Internet Protocol (VOIP) phone systems; acquisition of printers, scanners and copiers. If "Yes," this initiative is not required to complete the Project Approval Lifecycle. Please report this workload on the Agency Portfolio Report.	<input type="radio"/> Yes <input checked="" type="radio"/> No <input type="radio"/> Clear
5. Is the primary objective of the project to acquire desktop and mobile computing commodities as defined by SAM Section 4819.34, 4989? If "Yes," this initiative is a non-reportable project. Approval of the Project Approval Lifecycle is delegated to the head of the state entity. Submit a copy of the completed, approved Stage 1 Business Analysis to the CDT and track the initiative on the Agency Portfolio Report.	<input type="radio"/> Yes <input checked="" type="radio"/> No <input type="radio"/> Clear
6. Does the project meet all of the criteria for Commercial-off-the-Shelf (COTS) Software and Cloud Software-as-a-Services (SaaS) delegation as defined in SAM 4819.34, 4989.2 and SIMM 22 If "Yes," this initiative is a non-reportable project. Approval of the Project Approval Lifecycle is delegated to the head of the state entity; however, submit an approved SIMM Section 22 form to CDT.	<input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Clear
7. Will the project require a Budget Action to be completed?	<input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Clear
8. Is it anticipated that the project will exceed the delegated cost threshold assigned by CDT as identified in SIMM 10?	<input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Clear
9. Are there any previously imposed conditions place on the state entity or this project by the CDT (e.g., Corrective Action Plan)? If "Yes," provide the details regarding the conditions below.	<input type="radio"/> Yes <input checked="" type="radio"/> No <input type="radio"/> Clear
10. Is the system specifically mandated by legislation?	<input type="radio"/> Yes <input checked="" type="radio"/> No <input type="radio"/> Clear

Department of Technology Use Only

Original "New Submission" Date 3/1/2019

Form Received Date 3/1/2019

Form Accepted Date 3/1/2019

Form Status Completed

Form Status Date 3/1/2019

Form Disposition Approved If "Other," specify:

Form Disposition Date 3/1/2019