Note: Effective January 1, 2008, the Office of Information Security (Office) restructured and renumbered the content and moved SAM Sections 4840 – 4845 to SAM Sections 5300 – 5399. See also the Office's Government Online Responsible Information Management (GO RIM) Web site at https://cdt.ca.gov/security/ for statewide authority, standards, guidance, forms, and tools for information security activities.

CHAPTER 4900 INDEX

INFORMATION MANAGEMENT PLANNING

PURPOSE	**4900**
Basic Policies	**4900.2**
Agency Information Management Strategy Documentation	**4900.3**
Agency Information Management Strategy Reporting Requirements	**4900.5**
EXHIBITS AND SUPPORTING DOCUMENTS	**4903**
Information Management Organization	**4903.1**
Information Management Costs	**4903.2**
CONCEPTUALLY APPROVED IT PROJECT PROPOSALS REPORT	**4904**
ENTERPRISE ARCHITECTURE	**4906**
PROJECT MANAGEMENT	**4910**
Project Manager Qualifications	**4910.1**
California Project Management Framework (CA-PMF)	**4910.2**

PROJECT APPROVAL LIFECYCLE

PROJECT APPROVAL LIFECYCLE PURPOSE	**4920**
PROJECT APPROVAL LIFECYCLE BASIC POLICY	**4921**
PROJECT APPROVAL LIFECYCLE SCOPE	**4922**
PROJECT APPROVAL LIFECYCLE PARTICIPATION	**4923**
PROJECT APPROVAL LIFECYCLE DOCUMENTATION	**4924**
CONSISTENCY WITH AGENCY INFORMATION MANAGEMENT STRATEGY AND CONCEPTUALLY APPROVED IT PROJECT PROPOSALS REPORT	**4925**
PROJECT APPROVAL LIFECYCLE PROCESS	**4927**
PROJECT APPROVAL LIFECYCLE STAGE/GATE DELIVERABLES	**4928**

CHAPTER 4900 INDEX (Cont. 1)

IT PROJECT OVERSIGHT	**4940**
Independent Project Oversight Reports	**4940.1**
Corrective Action Plan	**4940.2**
Independent Verification And Validation	**4940.3**
COMPLIANCE REVIEW	**4942**
AUDIT OF INFORMATION TECHNOLOGY PROJECTS	**4943**
SPECIAL PROJECT REPORT – GENERAL REPORTING REQUIREMENTS	**4945**
Special Project Report – Content And Format	**4945.2**
MAINTENANCE AND OPERATIONS PLAN POLICY	**4946**
POST – IMPLEMENTATION EVALUATION REPORT	**4947**
Post – Implementation Evaluation Report – Content And Format	**4947.2**
TECHNOLOGICAL ALTERNATIVES – SELECTION CRITERIA	
INTRODUCTION	**4981**
Policy	**4981.1**
TECHNOLOGICAL ALTERNATIVES – DATA CENTERS	
INTRODUCTION	**4982**
Data Center Consolidation And Determination Of Agency - Data Center Assignments	**4982.1**
Policies For Data Center Management	**4982.2**
TECHNOLOGICAL ALTERNATIVES – CLOUD COMPUTING POLICY	
INTRODUCTION	**4983**
Policy	**4983.1**

(Continued)

CHAPTER 4900 INDEX (Cont. 2)

(Continued)

TECHNOLOGICAL ALTERNATIVES – OPEN SOURCE AND CODE USE

Introduction	**4984**
Policy	**4984.1**
Exceptions	**4984.2**

TECHNOLOGICAL ALTERNATIVES – DESKTOP AND MOBILE COMPUTING POLICY

DESKTOP AND MOBILE COMPUTING	**4989**
Definition Of Desktop And Mobile Computing	**4989.1**
Exclusions	**4989.2**
Agency/State Entity Roles And Responsibilities	**4989.3**
Policy Compliance	**4989.8**

PURPOSE **4900**
(Revised 6/2015)

Strategic planning is essential to the successful adoption of IT in state government. An Agency/state entity information management strategy provides a means of coordinating systems development throughout the Agency/state entity over the long term. It enables the Agency/state entity to build systems within a common infrastructure and recognizes that no investment in systems should be made without proper planning. Inherent in the concept of information strategy is the commitment to develop business systems that are based on the real business priorities of the Agency/state entity.

The purposes of the planning requirements in this section are to ensure that:

1. Agency/state entity plans for and uses of IT are closely aligned with Agency/state entity business strategies;
2. Each Agency/state entity identifies opportunities to improve program operations through strategic uses of IT; and
3. Each Agency/state entity establishes and maintains an IT infrastructure that supports the accomplishment of Agency/state entity business strategies, is responsive to Agency/state entity information requirements, and provides a coherent architecture for Agency/state entity information systems.

DEFINITIONS **4900.1**
(Reviewed 3/2011)

Agency Information Management Strategy. An agency's information management strategy is the agency's comprehensive plan for using information technology to address its business needs, i.e., to successfully carry out its programmatic mission. Ideally, the agency's information management strategy represents one aspect of a well-defined overall agency business strategy and is therefore closely aligned to its business strategy. If the agency has not established a business strategy, agency staff who are responsible for the agency information management strategy must make assumptions based on their knowledge of the agency's overall mission, its program resources and priorities, and the changing nature of its environment.

Business Strategy. An agency's business strategy is its overall plan for accomplishing its mission in a changing environment with the resources it can reasonably expect to be available. Such a strategy typically addresses the agency's statutory mission and historical role, the expectations of its key stakeholders (individuals and organizations that affect the agency or that the agency affects), the factors that are critical to its success as an organization, the agency's internal strengths and weaknesses, and the political, social, economic, and technological forces in its environment that support or constrain its programs. Business strategies articulate the key issues that must be successfully addressed by the agency and identify the priorities and required resources for proposed actions. A strategy may have a time frame that is as short as a few months, if there is a limited window of opportunity for significant change. However, most agency business strategies present a three- to five-year perspective, with some agencies finding it useful to extend their strategic vision as much as ten to twenty years into the future. Strategic planning is not a one-time effort; it is a fundamental, continuing management process that allows the agency to respond in an effective manner to a changing environment.

Information Technology Infrastructure. An agency's information technology infrastructure is the base or foundation for the delivery of information to support the agency's programs and management. The infrastructure contains elements upon which an agency's information technology activities are dependent. An agency must therefore define, implement, and manage these infrastructure elements to successfully employ information technology.

The desirable characteristics of this infrastructure are efficient support for the exchange of information within the agency and between the agency and other organizations; reliable availability of information processing capabilities whenever and wherever they are needed; preservation of the integrity and confidentiality of information maintained by the agency; sufficient flexibility to allow the timely and efficient addition of new information management capabilities and modifications of established capabilities; and consistency with a coherent set of technical and managerial standards for the employment of information technology.

(Continued)

(Continued)
DEFINITIONS **4900.1** (Cont. 1)
(Reviewed 3/2011)

Typical elements in an information technology infrastructure include:

Application Systems. The applications that an agency purchases and/or develops to achieve personal productivity and program support benefits.

Architecture. The guidelines or blueprints that an agency follows in designing, acquiring, and implementing information technology solutions. Organizationally approved definitions, specifications, and standards are the primary components in an agency's information technology architecture.

Communications. Local area and wide area network components, including linkages with other organizations.

Equipment. An agency's hardware platforms and components ranging from individual personal computers to mainframes and associated peripherals.

Facilities. The electrical, ventilation, fire suppression, physical security, wiring, and other components required to support an agency's information technology capability, including the physical structure itself.

Funding. Current and projected funding for information technology planning, acquisition, development, and operations activities.

Partnerships. Relationships with other public and private sector organizations that support and enable the agency's pursuit and use of information technology.

People. An agency's technical staff, user community groups, and executive steering and oversight committees that are charged with information technology planning, approval, development, management, operations, and security responsibilities.

Plans. Detailed designs or methods for aligning information technology activities with agency business strategies and accomplishing business objectives. Typical agency information technology plans include strategic, risk management, and operational recovery.

Policies. The rules, conventions, and protocols adopted by the agency to govern the pursuit and use of information technology.

Processes and Procedures. The defined steps for planning, approving, acquiring, developing, operating, maintaining, enhancing, and using information technology within the agency.

(Continued)

(Continued)
DEFINITIONS **4900.1** (Cont. 2)
(Reviewed 3/2011)

Service Definitions. The types of services provided, accepted service levels, and service delivery time frames established for an agency's information technology support organization.

Software. The set of operating system, utility, communications, user interface, and management programs that enable users to operate and control computers and develop application systems.

The infrastructure includes elements owned by the agency and available under contract or through interagency agreement. For agencies that employ the services of a consolidated data center, for example, the required data center resources are considered part of the agency's infrastructure.

Reengineering the Business Process. The search for, and implementation of, radical changes in business processes that result in dramatic efficiencies, reductions in turnaround time, improvements in quality, or improvements in customer service.

Strategic Planning Process for Information Technology. The process of aligning agency plans for, and uses of, information technology with the agency's business strategies.

BASIC POLICIES **4900.2**
(Revised 6/2015)

Each Agency/state entity must establish an ongoing strategic planning process for IT and submit its strategic plan to the California Department of Technology for approval. The strategic planning process established by an Agency/state entity should be consistent with its needs, resources, uses of IT, and management style. However, the strategic planning process should:

1. Be consistent with the current statewide strategic direction for IT, with relevant statewide policies contained in the State Administrative Manual, Statewide Information Management Manual and current management memos, and with Agency/state entity policies for the management of information and IT;
2. Include active participation of Agency/state entity executive and program management;
3. Align Agency/state entity strategies for IT with Agency/state entity business strategies;
4. Identify emerging threats and opportunities in the Agency/state entity's environment that have a potential impact on the Agency/state entity's information management and its use of IT;
5. Assess the strengths and weaknesses of the Agency/state entity in terms of its IT infrastructure and information management capabilities;
6. Assess the potential of new information technologies to enable new business strategies and further the accomplishment of established strategies;
7. Provide for the creation and maintenance of an Agency/state entity IT infrastructure that will support Agency/state entity information requirements and business strategies; and
8. Establish goals and priorities for the acquisition of new information management capabilities.

Each Agency/state entity may determine the format and content of the documentation of its strategic plan for IT. The documentation must satisfy Agency/state entity management requirements and be sufficiently detailed to provide the Department of Technology with a clear understanding of the Agency/state entity's information management strategy. Agency Information Management Strategy (AIMS) documentation guidelines can be found in SIMM Section 110.

(Continued)

(Continued)
BASIC POLICIES **4900.2** (Cont. 1)
(Revised 6/2015)

It is the responsibility of the Agency/state entity to ensure that the information available to the Department of Technology represents its current strategy. The Department of Technology will base its decisions regarding the approval of an Agency/state entity's IT activities and support for its budget augmentations in part upon its understanding of the Agency's Information Management Strategy (AIMS) and the relationship between the AIMS and the Agency/state entity's overall business strategy. In general, activities and proposals that are not supported by an AIMS that meets the basic requirements of this section or that are inconsistent with an Agency/state entity's established strategy will not be approved or supported by the Department of Technology. Any Agency/state entity that does not have an approved AIMS will have all IT project delegation rescinded, including delegation for expenditures under the Desktop and Mobile Computing Policy (SAM Section 4989.)

The Agency/state entity must submit documentation of its information management strategy to the Department of Technology at the time it completes its initial strategic planning effort and, thereafter, whenever there is a significant change in strategy. SAM Section 4900.3 provides guidelines for the AIMS documentation that must be submitted to the Department of Technology. Additionally, the Agency/state entity must annually certify that the AIMS approved by the Department of Technology represent its current strategy. See SAM Section 4900.5 and SIMM Section 60.

Note that approval of an Agency/state entity's AIMS does not imply approval of specific projects, nor does it guarantee funding for the plan or specific projects an Agency/state entity may initiate under the plan. Project funding must be addressed through the budget process, where final determination will be based on statewide as well as Agency/state entity priorities.

AGENCY INFORMATION MANAGEMENT STRATEGY DOCUMENTATION 4900.3

(Revised 6/2015)

Each Agency/state entity is expected to tailor the documentation of its information management strategy to its own needs and to provide the Department of Technology with sufficient information for the Department of Technology to understand that strategy in light of the Agency/state entity's overall business strategy. AIMS documentation guidelines can be found in SIMM Sections 60 and 110.

Agencies/state entities are requested to address at least the following in their submittal to the Department of Technology:

Changes in Mission and Programs. A summary of expected changes in the Agency/state entity's mission and programs that will require changes to the Agency/state entity's information management capabilities.

Agency Business Strategy. A summary of the Agency/state entity's business strategy for the period covered by the information management strategy.

Information Technology Vision. A summary of the Agency/state entity's values and principles that articulate the conceptual basis or foundation for the Agency/state entity's chosen IT infrastructure.

Impact on Information Management. An assessment of the impact of the Agency/state entity's business strategy upon its information management practices.

New Information Technologies. A statement of how new information technologies will be employed in the business strategy.

Current Information Technology Infrastructure. A description of key elements in the Agency/state entity's current IT infrastructure: standards, hardware, software, communications, personnel, partnerships, and application systems.

Planned Information Technology Infrastructure. A description of how that infrastructure will be developed or leveraged to meet future information requirements.

Information Management Priorities, Objectives, and Resources. A statement of the Agency/state entity's priorities, objectives, and resources for achieving the development or acquisition of new information management capabilities.

Activities to Reengineer Agency/state entity Business Processes. A description of changes the Agency/state entity has made, or is making, to restructure its business operations in an effort to achieve dramatic improvements in critical measures of performance, such as efficiency, turnaround time, customer satisfaction, and quality.

An Agency/state entity may prepare a separate summary of its information management strategy for submission to the Department of Technology or it may choose to provide the Department of Technology with copies of its internal documents. The Department of Technology may request additional information to clarify its understanding of an Agency/state entity's strategy. Agencies/state entities are encouraged to submit informational copies of their business strategies with their information management strategies and to provide oral briefings to the Department of Technology in conjunction with submitting their strategies.

AGENCY INFORMATION MANAGEMENT STRATEGY REPORTING REQUIREMENTS **4900.5**
(Revised 6/2015)

The AIMS must be submitted to the Department of Technology at the time the Agency/state entity completes its initial strategic planning effort. A revised AIMS must be submitted to the Department of Technology for approval whenever there is a significant change in the Agency/state entity's strategy. Additionally, to assist the Department of Technology in reviewing an Agency/state entity's IT Budget Change Proposals (see SAM Section 4819.42), the Agency/state entity annually must certify, by August of each year, or as instructed by the Department of Technology, that the AIMS approved by the Department of Technology represents its current strategy. SIMM Section 60 provides a template for the AIMS transmittal letter, which must be signed by the Agency/state entity director or chief deputy director, for this annual certification.

INFORMATION MANAGEMENT ORGANIZATION **4903.1**
(Revised 6/2015)

By June of each year, or as instructed by the Department of Technology in SIMM 05A, each Agency/state entity must submit to the Department of Technology organization charts showing:

1. The relationship between the organizational unit or units responsible for information management functions (including telecommunications) and other units within the Agency/state entity; and
2. The internal organization of the unit or units responsible for information management functions, including telecommunications. The internal organization chart should indicate numbers of positions by classification.

INFORMATION MANAGEMENT COSTS **4903.2**
(Revised 01/2017)

By February 1 of each year, or as instructed by the Department of Technology in SIMM 05A, each Agency/state entity is required to summarize its actual and projected information technology costs, telecommunications costs and information security costs (including the expenditure of federal grant funds for information security purposes), including, but not limited to, personnel, for the immediately preceding fiscal year and current fiscal year, showing current expenses and projected expenses for the current fiscal year.

The format and instructions for submittal required by the Department of Technology are specified in SIMM Section 55.

.

EXHIBITS AND SUPPORTING DOCUMENTS 4903

(Revised 6/2015)

The documents required in SAM Sections 4903.1-4903.4 supplement the information in the Agency/state entity AIMS by providing details about the organization or information management within the Agency/state entity and the resources available to the Agency/state entity.

CONCEPTUALLY APPROVED IT PROJECT PROPOSALS REPORT 4904

(Revised 10/2015)

To forge the necessary integration of the business and Information Technology (IT) functions in California state government, the California Department of Technology (Department of Technology) publishes a Conceptually Approved IT Project Proposals Report each quarter. The Report will be based on the approved Stage 1 Business Analyses from Agencies/state entities[1]. This information represents the Executive Branch's plan for IT investments in support of the California IT Strategic Plan. The information in the Conceptually Approved IT Project Proposals Report is used to:

- Ensure that IT investments drive program efficiency and effectiveness and improve the quality of government services for Californians.
- Facilitate improvements in internal business processes and financial management through IT investments.
- Link IT investments to Agency/state entity priorities and business direction.
- Promote the alignment of IT investments with the Agency/state entity's enterprise architecture (Technology, Standards, and Infrastructure).
- Enhance and promote enterprise data sharing through IT investments.
- Facilitate consideration and conceptual approval to pursue selected IT investments.

See SIMM Section 19A for Project Approval Lifecycle Stage/Gate deliverable Preparation Instructions.

---

[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.

ENTERPRISE ARCHITECTURE 4906

(Revised 6/2015)

The statewide Enterprise Architecture (EA) is developed in a cooperative, managed, and coordinated effort facilitated by the California Department of Technology. The National Association of State Chief Information Officers methodology and the Federal Enterprise Architecture framework included in SIMM Section 58A are adopted as the state's standards to develop and maintain the statewide EA.

Accordingly, Agencies/state entities shall implement EA in accordance with SIMM Section 58D. In addition, Agencies/state entities shall, to the extent practical, utilize the EA Practices included in SIMM Section 158.

PROJECT MANAGEMENT **4910**
(Revised 5/2016)

"Project management is the application of knowledge, skills, tools, and techniques to project activities to meet the project requirements. Project Management develops and implements plans to achieve a specific scope that is driven by the objectives of the program or portfolio it is subjected to and, ultimately, to organizational strategies." (PMBOK 5th Edition®). The purpose of project management is to ensure that the delivered product, service or result meets the customer's requirements and is delivered on time and within budget. A project management methodology improves the quality of project planning, communication, control of the execution and closure processes, and thus the deliverables. As the project progresses, and as challenges or changes emerge, the Project Manager must understand and balance the project's scope, schedule, cost, and quality objectives.

PROJECT MANAGER QUALIFICATIONS **4910.1**
(New 5/2016)

Agencies/state entities must assign Project Managers with the qualifications and skills commensurate with the complexity of the IT project they are managing. Assigning a skilled Project Manager is of critical importance to the success of IT projects. Project Management qualification requirements may be met through formal training, certification in industry stated project management, or previous experience. The following Project Manager qualification requirements are based on the project's Complexity Rating and assessed by the Department of Technology IT Project Oversight Division through the Project Approval Lifecycle:

Low Complexity Projects – The Project Manager should have some training in project management methodology and project management tools. In addition, the Project Manager should have demonstrated leadership, organization, critical thinking, and interpersonal skills.

Medium Complexity Projects – In addition to the requirements identified for low complexity projects, the Project Manager should have substantial project management training and experience leading several low complexity project efforts through all phases of the project lifecycle requiring the effective management of people and technology. The Project Manager should have proficiency in leadership, organization, critical thinking, stakeholder management, and Information Technology. Medium complexity projects typically incorporate more than one technology type or functional group, and the Project Manager needs to be able to manage several different functional groups with different needs.

High Complexity Projects – The Project Manager should possess advanced project management certifications and should have been directly responsible for all knowledge areas across all process groups for high-profile medium complexity project engagements and be well recognized for their efforts. The project manager must also have knowledge of various approaches to system development/replacement, procurement, contract management, personnel management, supplier management, stakeholder management, operation support, and Organizational Change Management. A project manager at this level must be able to understand the technology being used but not necessarily be an expert in it. Project managers will be spending most of their time working the planning and controlling aspects of the project as well as dealing with the "political" issues. Delegation, time management, and interpersonal skills are keys to success. Large complexity projects are those that are Agency/state entity-wide or extend beyond the Agency/state entity itself. The person must have the unwavering confidence of Agency/state entity management and be considered an acceptable and respected representative for the Agency/state entity.

(Continued)

(Continued)
PROJECT MANAGER QUALIFICATIONS **4910.1** (Cont. 1)
(New 5/2016)

The AIO or the Department CIO, as appropriate, is responsible for ensuring that project managers possess the appropriate qualification before their assignment to an IT project. The Department of Technology may require, at any time, the Agency/state entity to provide evidence of the Project Manager's certification, training or previous project management experience.

CALIFORNIA PROJECT MANAGEMENT FRAMEWORK (CA-PMF) 4910.2
(New 5/2016)

The California Project Management Framework (CA-PMF) has been designed as an adaptable resource that provides California public sector organizations with an approach to project management that lays the foundation for project success. The CA-PMF offers guidance and insight on project management methods and approach through the use of scalable resources, tools, and templates. The CA-PMF is intended as a practical and useful guide to lead a Project Manager and project team through the project management lifecycle for projects of all sizes so that they achieve expected outcomes. The framework supports project management practices that conform to industry standards as defined by the Project Management Institute (PMI) and adapted to the context of California State government.

The CA-PMF includes all major project processes and activities, from initial project definition to closing the project. With project management described as a series of activities undertaken by the project team, the Project Manager is equipped with the tools necessary to consider the needs of the project and how its organization can be structured and managed to deliver the intended result. The CA-PMF aligns with policy, identifies the connections to the project oversight and project approval processes, and directs practitioners to the appropriate resources for further information on those processes.

PROJECT APPROVAL LIFECYCLE PURPOSE **4920**
(Revised 6/2015)

The Project Approval Lifecycle (PAL) represents an opportunity for Agency/state entity's management to assess the full implications of a proposed IT project. The PAL is also the means of linking a specific IT project to the Agency/state entity's strategic business plans and IT plans, and to ensure that the proposed project makes the best use of the Agency/state entity's IT infrastructure. The PAL is divided into four stages, separated by gates (business analysis, alternatives analysis, procurement analysis and solution analysis). Each stage consists of a set of prescribed, cross-functional, and parallel activities to develop deliverables used as the inputs for the next stage. The gates provide a series of "go/no go" decision points that request only the necessary and known information needed to make sound decisions for that particular point in time. As additional information is collected and refined through the lifecycle, the cost estimates, schedules, and business objectives will be progressively updated and evaluated to determine if the project is still practical and if the investment should continue to move forward towards project approval. The model also integrates procurement into the project approval lifecycle, providing better estimates regarding a project's budget and schedule. The purpose of the PAL is to accomplish the following:

1. Better business outcomes for the State through successful IT projects.
2. Result in more successful projects and fewer Special Project Reports.
3. Improve efficiencies through effective project planning and analysis to meet State business needs, while also ensuring compliance with State IT policies.
4. Introduce scalability to the project approval process based on business and/or technical complexity.
5. Ensure each decision point requires only the necessary and appropriate level of information needed to make a sound decision, estimate, or product for that particular stage.
6. Determine whether there is a substantiation for a proposed project, i.e., whether the expenditure of public resources on the project is justified based on the following:
    a. Responsiveness to a clearly-defined, program-related problem or opportunity;
    b. Selection of the best of the possible alternative;
    c. Agency/state entity's technical and program capabilities; and
    d. Financial and/or non-financial benefits over the life of the solution that exceed development and operations costs. Project benefits typically include reduced program costs, avoidance of future program cost increases, increased program revenues, or provision of program services that can be provided most effectively through the use of IT.

(Continued)

7. Provide a means for achieving agreement between Agency/state entity's executive management, program management, and project management regarding:
    a. The scope, benefits, schedule, and costs of a proposed project;
    b. Management responsibilities over the course of the project; and
    c. Opportunities to collaborate with the Department of Technology.
8. Provide executive branch control agencies and the Legislature with sufficient information to assess the merits of the proposed project and determine the nature and extent of project oversight requirements.
9. To the extent feasible, ensure each step and work product in the lifecycle is useful input into subsequent steps.
10. Ensure that a "no" or a "go back and re-think" decision is communicated as early as possible if the level of detail provided is inadequate.

PROJECT APPROVAL LIFECYCLE BASIC POLICY 4921

(Revised 11/2016)

Project Approval Lifecycle (PAL) Stage/Gate deliverables must be reviewed and approved in accordance with the general requirements of SAM Sections 4819.3-4819.42 (State Information Management Authority and Responsibility), as well as the specific requirements of Sections 4927-4928. See SIMM Section 19 for PAL Stage/Gate deliverable Preparation Instructions.

PROJECT APPROVAL LIFECYCLE SCOPE 4922

(Revised 6/2015)

The scope of the Project Approval Lifecycle (PAL) Stage/Gate deliverables must be commensurate with the nature, complexity, risk, and expected cost of the proposed use of IT.

The deliverables must provide sufficient information to assure the Agency/state entity's program management that the proposed response meets program requirements. The deliverables must also provide sufficient information to allow Agency/state entity executive management to make a sound decision as to the merits of the proposed project as an investment of public resources.

PROJECT APPROVAL LIFECYCLE PARTICIPATION 4923

(Revised 6/2015)

The analysis performed in support of Project Approval Lifecycle Stage /Gate deliverables must be based on an understanding of the needs, priorities, and capabilities of: (1) the users of the information that is to be provided; and (2) the Agency/state entity's unit or program that will have operational responsibility for the IT application. Representatives of program management and staff must be the business owners and drive the deliverable development process. Refer to SIMM Section 19.

PROJECT APPROVAL LIFECYCLE DOCUMENTATION 4924

(Revised 6/2015)

The SAM Section 4928 and instructions and guidelines published by the California Department of Technology (see SIMM Section 19) specify the content of the Project Approval Lifecycle (PAL) Stage/Gate deliverables which must provide the results of the analysis performed. In addition to the PAL Stage/Gate deliverables, the Agency/state entity must maintain sufficient supporting documentation to ensure that project participants, Agency/state entity management, and control agency personnel can resolve any questions that arise with respect to the intent, justification, nature, and scope of the project.

CONSISTENCY WITH AGENCY INFORMATION MANAGEMENT STRATEGY AND CONCEPTUALLY APPROVED IT PROJECT PROPOSALS REPORT 4925

(Revised 11/2016)

Each proposed project must be consistent with the Agency/state entity's overall strategy for the use of IT, as expressed in its current Agency Information Management Strategy (see SAM Sections 4900.2, 4900.3 and 4900.5.) and Conceptually Approved IT Project Proposals Report (see SAM Section 4904).

PROJECT APPROVAL LIFECYCLE PROCESS 4927

(Revised 08/2016)

Each Agency/state entity must follow a systematic, analytical process for evaluating and documenting the analysis of proposed IT projects, as defined in SAM Section 4819.2. This process includes:

1. Developing an understanding of a problem (or opportunity) in terms of its effect on the Agency/state entity's mission and programs;
2. Developing an understanding of the organizational, managerial, and technical environment within which a response to the problem or opportunity will be implemented;
3. Establishing programmatic and administrative objectives against which possible responses will be evaluated;
4. Preparing concise solution requirements of an acceptable response;
5. Identifying and evaluating possible alternative responses with respect to the established objectives;
6. Preparing an financial analysis for each alternative that meets the established objectives and solution requirements;
7. Selecting the alternative that is the best response to the problem or opportunity;
8. Developing a solicitation package that will result in the selection of qualified vendors;
9. Developing a contract by which the state and the vendor can effectively leverage to achieve project objectives and outcomes;
10. Preparing a management plan for implementation of the proposed response;
11. Capturing and documenting the results of the study in the form of analytical and comparable data in the Project Approval Lifecycle Stage/Gate deliverables, as specified in SAM Section 4928;
12. Validating the maturity and readiness of the Agency/state entity to undertake critical project activities (e.g., testing, release management, organizational change management, business process reengineering);
13. Reinforcing the commitment of stakeholders, state staff, and contractor/vendor resources prior to project design, development and implementation; and
14. Establishing accurate and realistic baselines to measure project health and success.

PROJECT APPROVAL LIFECYCLE STAGE/GATE DELIVERABLES **4928**
(Revised 08/2016)

The Project Approval Lifecycle (PAL) Stage/Gate deliverables, here and after referred to as "deliverables", must provide an accurate summary of the results of each Stage/Gate analysis. The deliverables must provide a complete summary of the results of the analysis and establish the business case for investment of state resources in a proposed project by setting out the reasons for undertaking the project and analyzing its costs and benefits. The PAL Stage/Gate model includes the following deliverables:

Stage 1 Business Analysis: Provides a basis for project management, program management, executive management, and state-level control agencies to understand and agree on business problems or opportunities, and the objectives to address them. In order to evaluate a Stage 1 Business Analysis, the Department of Technology must fully understand the business justification. Therefore, each proposal must describe in detail the business driver(s), statutes or legislation, program background and context, business problems or opportunities, strategic business alignment, organizational readiness, and business and stakeholder impact. Additionally, the Stage 1 Business Analyses are used to generate the quarterly Conceptually Approved IT Project Proposals Report which represents the Executive Branch's plan for IT investments in support of the California IT Strategic Plan.

Stage 2 Alternatives Analysis: Provides a basis for how the proposal's business objectives will be achieved, the evaluation of multiple alternative solutions, determines which alternative will yield the highest probability of meeting the business objectives, and to develop an acquisition strategy/plan for procuring services. In order to evaluate a Stage 2 Alternatives Analysis, the Department of Technology must fully understand how the selected alternative will best achieve the proposed project's business objectives. Each proposal must provide sufficient detail to describe the baseline processes, mid-level solution requirements, alternative solutions, recommended solution, procurement strategy and staffing considerations. This deliverable must also include a financial analysis of the life cycle costs, benefits and source of funding of the proposed project and the costs and benefits of the current method of operation during the life cycle of the project.

(Continued)

(Continued)
PROJECT APPROVAL LIFECYCLE STAGE/GATE DELIVERABLES **4928** (Cont. 1)
(Revised 08/2016)

Stage 3 Solution Development: Provides a basis for how the project will mature mid-level solution requirements into clearly defined and detailed solution requirements, develop solicitations to acquire solutions that best meet business objectives and yield the highest probability of success. In order to evaluate a Stage 3 Solution Development, the Department of Technology must fully understand the procurement methodology, approach and selection criteria to obtain a value effective solution. Each proposal must provide sufficient detail to describe the procurement profile, solution requirements, evaluation criteria, cost and payment model, negotiation strategy, statement of work, and staffing plan.

Stage 4 Project Readiness and Approval: Provides a basis for how the intended awardee will contribute towards the successful achievement of the project's business objectives and yield the highest probability of success, ensure the Agency/state entity's readiness to execute the project and establish realistic schedule and cost baselines. In order to evaluate a Stage 4 Project Readiness and Approval, each proposal must provide sufficient detail to describe the solicitation results, contract management strategy, organizational/project readiness and project baselines (scope, schedule, cost and resources). This deliverable must also include an updated financial analysis which will support the final approval of project funding requests.

PAL Stage/Gate deliverables must be submitted to the California Department of Technology (Department of Technology), and to the Office of the Legislative Analyst, and to the Department of Finance's Information Technology Consulting Unit. Deliverables must be submitted in a format specified by the Department of Technology and signed by the Agency/state entity director or his/her designee. The Department of Technology publishes detailed instructions and guidelines for Agency/state entity use in preparing deliverables. A copy of the instructions, guidelines, and required forms is available in SIMM Section 19. The instructions and guidelines specify the MINIMUM amount of information necessary for the Department of Technology's approval.
The Agency/state entity must maintain sufficient documentation of each analysis to ensure that project participants, Agency/state entity management, and control agency personnel can resolve any questions about the intent, justification, nature, and scope of the project.

PROJECT SUMMARY PACKAGE 4930

(Revised 7/2014)

A Project Summary Package must be prepared and included in each Feasibility Study Report and Special Project Report. In addition, the Project Summary Package may be used to document the feasibility study for projects with a total development cost equal to or less than ten percent of the Agency/state entity's cost delegation threshold. See SAM Section 4819.39.

See SIMM Section 20 and/or 30 for instructions for completing the Project Summary Package.

IT PROJECT OVERSIGHT 4940

(Renamed and Revised 04/2017)

Department of Technology project oversight is required for all Reportable Information Technology (IT) projects, unless otherwise exempted by the Department of Technology. IT Project Oversight is required to begin on the proposed project start date as identified in the Stage 4 approval letter and must continue through the duration of the project unless other direction is issued by the Department of Technology. Agency/state entity management must comply with IT Project Oversight Framework (see SIMM Section 45) throughout all project phases to ensure the appropriate level of independent project oversight, project management practices and project risk assessments. Compliance with the IT Project Oversight Framework may be required to begin as early as the Stage 3 Solution Development, as a condition of Stage 2 Alternatives Analysis approval.

The Department of Technology will conduct Agency/state entity, IT project management and oversight assessments designed to provide Agency/state entity management and the Department of Technology information on the progress of a project, including compliance with the minimum requirements for IT project management, project risk management, project oversight and project reporting activities at the Agency/state entity and control agency levels as outlined in the IT Project Oversight Framework (see SIMM Section 45). The Department of Technology will schedule assessments based on an established criteria.

The fundamental requirements for project oversight and evaluation are specified in SAM Sections 4819.31-4819.42. All projects, including projects delegated by the California Department of Technology to the Agency/state entity director, are subject to these review, reporting and evaluation requirements including the requirements of SAM Section 4940. Projects that have been delegated to the Agency/state entity director in accordance with SAM Section 4819.36 require appropriate project reporting by the project manager to the Agency/state entity director. Project oversight services contracted by Agency/state entities or the Department of Technology must comply with the IT Project Oversight Framework (see SIMM Section 45) and the requirements outlined in SAM Section 4910. The Department of Technology may conduct assessments to ensure compliance with minimum requirements.

INDEPENDENT PROJECT OVERSIGHT REPORTS 4940.1

(New 04/2017)

Independent Project Oversight Reports (IPORs) are used to detail a project's progress against the project objectives, scope, schedule, and cost defined in approved Project Approval Lifecycle documents. IPORs must be completed by the Department of Technology IPO Manager, who shall identify and quantify any issues and risks affecting project objectives. IPORs are required to be developed regularly based on project criticality (see SIMM Section 45).

CORRECTIVE ACTION PLAN 4940.2

(New 04/2017)

Based on the Independent Project Oversight Report (IPOR) findings, the California Department of Technology (Department of Technology) may require Agency/state entities to develop a Corrective Action Plan (CAP) for the purpose of altering the course of a task or project that may have significantly deviated from the pre-specified direction originally intended. The CAP must be well-documented and, upon approval by the Department of Technology, be executed to get the project back on track to better align with the goals, expectations, and ultimate results laid out in the Project Approval Lifecycle and/or project management plan.

The Department of Technology will actively monitor the progress of the planned remediation actions outlined in the approved CAP and document the independent assessment in the IPOR. If the Department of Technology determines that the Agency/state entity is not effectively implementing the actions outlined in the CAP, the Department of Technology may take action to further escalate any lack of progress and adherence to the CAP. If those escalation efforts fail to correct significant problems related to specified issues or risks, the Department of Technology will continue escalation activities up to and including IT project suspension or termination.

INDEPENDENT VERIFICATION AND VALIDATION 4940.3

(New 04/2017)

Independent Verification and Validation (IV&V) is the process for ensuring that a product, service, or system meets requirements and specifications and that it fulfills its intended purpose. Within IV&V, the term verification refers to the process of evaluating software to determine whether the products of a given development phase satisfy the conditions imposed at the start of that phase. [IEEE-STD-610]. The term validation refers to the process of evaluating software during or at the end of the development process to determine whether it satisfies specified requirements. [IEEE-STD-610]. IEEE–STD-1012 industry standards will be used to guide the IV&V activities.

When contracting for IV&V services, Agencies/state entities must use the standard Statement of Work (SOW) template (see SIMM Section 45A). Any changes to the standard SOW template requires approval by the California Department of Technology.

The following IV&V requirements apply to all reportable projects, based on the project criticality rating assigned by the Department of Technology:

- IV&V services are required for all reportable projects classified as medium or high criticality and must begin on or before the proposed project start date as identified in the Stage 4 approval letter issued by the Department of Technology and must continue through the duration of the project unless other direction is provided by the Department of Technology.
- IV&V services may be required for projects classified as low criticality at the discretion of the Agency Chief Information Officer (AIO) or the Department of Technology.
- IV&V services may be required during the Project Approval Lifecycle, as directed by the Department of Technology.
- To ensure independence, IV&V services for Agency-affiliated State Entity projects must report to the respective AIO.
- A single vendor may not provide both IV&V and Independent Project Oversight services for the same project.

OVERVIEW **4941**

(Removed 04/2017)

Information previously contained in this section has been consolidated into SAM section 4940.

COMPLIANCE REVIEW 4942

(Revised 7/2014)

Specific projects or Agencies/state entities as a whole may be subject to compliance reviews conducted by the California Department of Technology (Department of Technology). The purposes of a compliance review are to verify Agency/state entity adherence to statewide IT policies as well as approved Agency/state entity policies, and to determine Agency/state entity fulfillment of approved plans. The Department of Technology will review project reporting documentation in conjunction with its compliance review and oversight responsibilities.

The Department of Technology may impose sanctions, such as a reduction or elimination of an Agency/state entity's delegated cost threshold for reporting and approval of IT projects by the Department of Technology, or other sanction deemed appropriate by the Department of Technology, upon finding that an Agency/state entity is consistently and/or willfully out of compliance with state policies.

AUDIT OF INFORMATION TECHNOLOGY PROJECTS 4943

(Revised 6/2015)

All information technology (IT) projects are subject to audit, with project reporting and evaluation documents an essential aspect of the audit trail. Documentation supporting project decisions must be kept by the Agency/state entity for a minimum of two years following approval of the post-implementation assessment.

Some projects may be subject to ongoing review by the Department of Finance's Office of State Audits and Evaluations (OSAE). OSAE may review the Project Approval Lifecycle Stage/Gate deliverables of projects approved by the California Department of Technology (Department of Technology) and the Reporting Exemption Requests of projects delegated to agencies by the Department of Technology. OSAE will select projects for ongoing review based on their risk, cost, and materiality.

For projects selected for ongoing review, OSAE will develop and submit to Agency/state entity management periodic status reports and the project Post-Implementation Evaluation Report (PIER) required under SAM Section 4947. Agencies/state entities are required to submit final versions of the periodic status reports and the project PIER to the Department of Technology within five working days after they are received from OSAE.

If OSAE determines that the project should be audited, the Agency/state entity must enter into an interagency agreement with OSAE for that purpose. Since the cost that the Agency/state entity otherwise would have incurred in monitoring the project and producing progress reports and the PIER will no longer be borne by the Agency/state entity, these costs should not be included in the project budget. However, the Agency/state entity should ensure that the project budget includes an amount sufficient to cover the costs of the interagency agreement with OSAE.

IT PROJECT OVERSIGHT AND REPORTING 4944

(Removed 04/2017)

Information previously contained in this section has been consolidated into SAM section 4940.

SPECIAL PROJECT REPORT-
GENERAL REPORTING REQUIREMENTS 4945

(Revised 6/2015)

Preparation of an Special Project Report (SPR) is required whenever a project substantially deviates from the costs, benefits or schedules documented in the approved Stage 4 Project Readiness and Approval, when a major revision occurs in project requirements or methodology, when criteria listed in SAM Section 4819.37, other than the project's cost exceeding the level the California Department of Technology (Department of Technology) may have delegated to the Agency/state entity, arise during the development or implementation of the project, or when a significant change in state policy draws into question the assumptions underlying the project. No encumbrance or expenditure of funds shall be made to implement an alternative course of action until approval has been received from the Department of Technology or the Agency/state entity director, as appropriate. SAM Section 4819.36 lists specific conditions that require submission of an SPR to the Department of Technology.

If an SPR for a delegated project must be submitted to the Department of Technology, the Agency/state entity must attach to the SPR a copy of the approved Feasibility Study Report or all approved Project Approval Lifecycle Stage/Gate deliverables and the Transmittal signed by the Agency/state entity director or his/her designee.

The SPRs which must be submitted to the Department of Technology should be transmitted within 30 days after recognition of a substantial deviation. The SPR must be submitted to the Department of Technology and the Office of the Legislative Analyst. SPRs must be submitted in a format specified by the Department of Technology and signed by the Agency/state entity director or the director's designee. See SIMM Section 30 for SPR Preparation Instructions.

SPECIAL PROJECT REPORT-CONTENT AND FORMAT 4945.2

(Revised 6/2015)

The Special Project Report (SPR) must provide sufficient information for Agency/state entity management, executive branch control agencies, and the Legislature to assess the merits of the proposed project change and determine the nature and extent of future project oversight requirements. If an SPR lacks sufficient information for these purposes, the California Department of Technology (Department of Technology) will request that the Agency/state entity provide additional information.

Information provided in the SPR must be commensurate with the level of deviation of costs, benefits, timelines, or project requirements from those of the approved FSR, Stage 4 Project Readiness and Approval or last approved SPR.

The SPRs must be submitted in a format specified by the Department of Technology and signed by the Agency/state entity director or his/her designee. The MINIMUM content for an SPR is project status, an explanation of the reason for the project deviation, a revised project management schedule, and financial summary information. The Department of Technology publishes instructions and guidelines for Agency/state entity's use in preparing SPRs. See SIMM Section 30 for SPR Preparation Instructions.

MAINTENANCE AND OPERATIONS PLAN POLICY 4946

(Revised 6/2015)

The Maintenance and Operations (M&O) Plan provides an orderly, cost effective and planned process for ongoing routine M&O activities of implemented IT systems.

The California Department of Technology (Department of Technology) may request Agencies/state entities to submit an M&O Plan for IT projects. Agencies/state entities requested to submit an M&O Plan must have the plan approved by the Department of Technology before commencing M&O activities. Once an M&O Plan is approved, Agencies/state entities must provide the Department of Technology annual updates. The Department of Technology can suspend or withdraw its approval of the M&O Plan to respond to changing circumstances.

See SIMM Section 160 Maintenance and Operations Plan Guidelines.

POST-IMPLEMENTATION EVALUATION REPORT 4947

(Revised 04/2017)

A post-implementation evaluation report (PIER) must be prepared by the Agency/state entity following the completion of each IT project, unless the Agency/state entity has entered into an interagency agreement with the Department of Finance's Office of State Audits and Evaluations (OSAE) under SAM Section 4943. The PIER shall:

1. Measure the benefits and costs of a newly-implemented IT application or system against the most recently approved project objectives; and
2. Document projected operations and maintenance costs over the life of the application or system.

No project is considered complete until the PIER has been approved by the Department of Technology or by the Agency/state entity director, as appropriate. Approval of a PIER by the Department of Technology or the Agency/state entity director, as appropriate, terminates the project reporting requirements.

If OSAE selects the project for review under SAM Section 4943, OSAE will conduct the post-implementation assessment and submit the PIER to Agency/state entity management. The Agency/state entity is required to submit the PIER to the Department of Technology within five working days after it is received from OSAE.

The post-implementation assessment must be conducted after the new IT capability has been operational for a sufficient period of time for its benefits and costs to be accurately assessed. Initial operational problems must have been resolved and sufficient experience and data must have been accumulated to determine whether the project met the proposed objectives, was completed within the anticipated time and budgetary constraints, and achieved the proposed benefits. The optimum time after implementation to conduct the assessment depends upon the nature of the project. Six months to one year after implementation is typical. The assessment MUST be completed within 18 months of project completion. Agencies/state entities are required to follow the instructions for preparing and submitting the PIER and Transmittal Letters, see SIMM Section 50.

POST-IMPLEMENTATION EVALUATION REPORT-CONTENT AND FORMAT 4947.2

(Revised 6/2015)

The Post Implementation Evaluation Reports (PIERs) must be submitted in a format specified by the California Department of Technology (Department of Technology) and signed by the Agency/state entity director or his/her designee, see SIMM Section 50. The level of detail included in the PIER must be commensurate with the scope and complexity of the project and its anticipated benefits. The narrative portion of the PIER for a minor project can be as brief as one or two pages. However, it must provide sufficient information for Agency/state entity management, executive branch control agencies, and the Legislature to assess the success of the project. In particular, the PIER must contain a comparison of the timelines, costs and benefits forecast by the approved FSR or Project Approval Lifecycle Stage/Gate deliverables with the actual timelines, costs and benefits of the project. If the project was a limited success or involved significant differences between expectations and results, the Agency/state entity must present the actions it intends to take to improve the outcome. If the project was a failure and the problem or opportunity that led to the project still exists, the Agency/state entity must present the actions it intends to take to address that problem or opportunity.

INTRODUCTION 4981

(Reviewed 6/2015)

No single combination of information technology (IT) and management philosophy can be identified as being universally suitable for state government, nor can pre-determined rules be established to allow the routine assignment of a new application to the particular combination of technology and management practice which will be most appropriate. Each decision regarding a choice of IT and management structure must be made on a case-by-case basis, considering the particular circumstances of the application and the particular technological and managerial options available.

POLICY **4981.1**
(Revised 6/2015)

The decision to select a particular technological approach must take into account the full range of significant factors which will influence the success of the application during its operational life. These significant factors include:

1. **Statutes, Regulations and Policies**-This factor consists of applicable statutes, regulations and policies which could impact a decision to use IT.
2. **Agency/state entity Management**-This factor includes assessment of the Agency/state entity's prior experience with IT and the managerial resources it can bring to bear on the use and control of the technology, i.e., whether the Agency/state entity has an appropriate management infrastructure and Agency/state entity personnel possess the necessary qualifications.
3. **Cost**-Applications of IT must be reviewed in terms of their cost justification. Such review must take into account the potential impact of the application on the overall economy of state operations. Assessment of the costs associated with each technological alternative must cover a sufficient time span to allow for reasonable amortization of start-up costs as well as realization of cost savings and cost avoidance potentials.
4. **Nature of the Application**-This factor encompasses (1) the extent to which the application is critical to the accomplishment of the Agency/state entity's mission, goals and objectives, (2) the degree of centralization or decentralization required for this activity, (3) the data communication requirements associated with the activity, (4) the characteristics of the data to be collected and processed, i.e., source, volume, volatility, distribution, and security or confidentiality, (5) the urgency of the application, and (6) backup requirements for personnel, software, data and hardware.
5. **Hardware Considerations**-This factor includes review of the alternative hardware configuration options capable of effecting the successful implementation of a given IT activity. Consideration must be given to (1) compatibility with existing hardware, including telecommunications equipment, (2) physical plant requirements necessary for proper operation of the equipment, (3) hardware maintenance, (4) the knowledge and skills required of state personnel, (5) backup processing capability, and (6) the existing capacity, immediate required capacity and future capacity.

(Continued)

6. **Software Considerations**-This factor includes a review of the software options available to achieve successful implementation of a given IT activity. Consideration must be given to (1) the compatibility of computer languages with existing and planned activities, (2) maintenance of the proposed software, e.g. vendor-supplied, (3) the urgency of the application, (4) the knowledge and skills required of state personnel, (5) the availability of complete documentation, and (6) the availability of necessary security features.
7. **Interagency Considerations**-This factor includes analyzing the Agency/state entity's interfaces with other Agencies/state entities, or federal or local government. Consideration must be given to compatibility of communications and sharing of data.

INTRODUCTION 4982

(Revised 1/2016)

Government Code Section 11534 and 11790 define two consolidated data centers in state government: 1) the Hawkins Data Center in the Department of Justice, and 2) the Office of Technology Services in the California Department of Technology. Other data processing centers are considered single-Agency/state entity, dedicated-use data processing centers rather than consolidated data processing centers. All data centers shall adhere to the following center policies.

DATA CENTER CONSOLIDATION AND DETERMINATION OF AGENCY-DATA CENTER ASSIGNMENTS 4982.1

(Revised 6/2015)

It is the state's policy to transition out of non-Tier III data centers and server rooms and to end upgrades during the transition, unless there is an emergency. The following policy shall be used to determine an Agency/state entity's Tier III-equivalent facility assignment for services, and to ensure consolidation activities proceed timely:

1. The Hawkins Data Center shall serve as the Tier III-equivalent for the Department of Justice. Agencies/state entities assigned to other state-designated Tier III-equivalent facilities whose official business requires access to the data contained in the California Criminal Justice Information System's (CJIS) data repositories, including those Agencies/state entities utilizing the California Law Enforcement Telecommunications System (CLETS), shall access CJIS serviced data repositories and CLETS through the Hawkins Data Center.
2. The Department of Water Resources Data Center serves as the Tier III-equivalent facility for the Natural Resources Agency and its associated Agencies/state entities.
3. The Franchise Tax Board (FTB) Data Center serves as the Tier III-equivalent data center for the FTB.
4. The following Office of Technology Services (OTech) facilities shall serve as the Tier III-equivalent Data Centers for all other Agencies/state entities in the state:
    a. The OTech Gold Camp Data Center serves as the production data center for the Executive Branch. In addition, the Gold Camp Data Center manages services and provides disaster recovery services to all state agencies not identified in 1, 2, and 3 above.
    b. The Federal Data Center (FDC) located at the OTech Gold Camp facility serves as a physically partitioned-off Data Center shared by agencies.
    c. The OTech Vacaville Data Center serves as a disaster recovery site with a secondary role as a production data center.
    d. Any other Tier III-equivalent facility designated by the Department of Technology.

(Continued)

(Continued)
DATA CENTER CONSOLIDATION AND DETERMINATION OF AGENCY-DATA CENTER ASSIGNMENTS **4982.1** (Cont. 1)
(Revised 6/2015)

5. To facilitate timely completion of consolidation activities:
    a. The OTech Customer Owned Equipment Managed Services (COEMS) is discontinued. COEMS customers will transition to one of the state's Tier III-equivalent facilities previously referenced.
    b. Agency/state entity server rooms will be closed.
    c. File and print services in the greater Sacramento area will be consolidated.
    d. New applications, server refreshes, storage replacements, and new virtualization clusters shall be located at a state Tier III-equivalent facility.
    e. Agencies/state entities shall review all IT projects that are in progress in order to plan transition of servers and storage to a state Tier III-equivalent facility.
    f. The Computer Room Construction policy and requirements established in Technology Letter 12-05 remain in effect.
    g. Facility upgrades for server rooms designated for shutdown will be limited to emergencies. Agencies/state entities shall utilize the approval procedures described in Technology Letter 12-05.
6. Agencies shall use the Data Center Consolidation Survey and Assessment (S&A) included in SIMM Section 67, and will be reporting to the Department of Technology, Information Technology Project Oversight Division (ITPOD) in accordance with the timeframes and submittal instructions included in SIMM Section 05A.

POLICIES FOR DATA CENTER MANAGEMENT **4982.2**
(Revised 6/2015)

Data Center Mission–Each data center shall have a statement of mission which states the data center's objectives and outlines the services provided by the center.

Data Center User Interaction–

1. Each data center shall have a functional responsibility to provide liaison with the users of the center. This shall include establishing and maintaining user groups and forums appropriate to the requirements of the users and the mission of the center.
2. Each data center shall make readily available a data center user guide which shall contain detailed and up-to-date descriptions of and instructions for the use of the various services offered by the center. This guide should describe the operational management processes required by user Agencies/state entities to avail themselves of data center services including resources scheduling, problem management, system backup and recovery procedures and data communications network management.

Data Center Financial Management–See SAM Section 6780 for the financial management policy applicable to the Office of Technology Services.

Exchange of Data Between Data Centers–The exchange or transfer of data between data centers by intercoupling or telecommunications shall be made only with the approval of the Department of Technology. Requests for approval to exchange or transfer data between data centers must contain programmatic justification and describe how the exchange or transfer will be accomplished. The request must also clearly describe what safeguards will be established to provide data confidentiality and security in compliance with SAM Sections 5300-5399, State Information Security Policy.

This section does not prohibit the transmission of data from the Department of Motor Vehicles to the Hawkins Data Center in order to obtain vehicle registration and driver license data for criminal justice purposes, or the transmission of data between centers in the same Agency/state entity.

INTRODUCTION 4983

(Revised 08/2017)

Cloud Computing is an effective method for the secure, agile and reliable delivery of government services in the State of California. Cloud computing enables business programs to enhance service delivery while ensuring the underlying technologies are transparent, ubiquitous, and interchangeable. To harness the benefits of cloud computing, the State of California has adopted this Cloud Computing Policy. This policy is intended to accelerate the pace at which Agencies/state entities will realize the benefits of cloud computing while adequately addressing relevant statutory and policy requirements associated with State IT systems, including information security and risk management, privacy, legal issues, and other applicable requirements.

POLICY **4983.1**
(Revised 08/2017)

As part of the Cloud Computing policy, each Agency/state entity shall:

1. Evaluate, in consultation with their IT organization, secure cloud computing alternatives for all IT projects and infrastructure initiatives (e.g., storage, servers, and Wide Area Network equipment).
2. Use a cloud service model, i.e., Software as a Service (SaaS), Platform as a Service (PaaS), or Infrastructure as a Service (IaaS), whenever a feasible and cost effective solution is available. The use of cloud services must be consistent with the factors described in SAM 4981.1.
3. Use IaaS or PaaS solutions for new, expansion or refresh initiatives.
4. Use IaaS and PaaS solutions provided through the California Department of Technology (CDT). Requests shall be submitted to CDT through a Remedy Service Request.
5. If required IaaS or PaaS solutions are not available through CDT, CDT will partner with the Department of General Services (DGS) to determine the best procurement method.
6. Use SaaS solutions provided through CDT, e.g., all office productivity software (including email*), or through DGS' Software Licensing Program (SLP), when implementing commercial and/or government SaaS cloud computing solutions.

   *Per Chapter 404, Statutes of 2010 (Assembly Bill 2408), all Agencies/state entities within the executive branch that are under the direct authority of the Governor must consolidate to the state's share e-mail solution.
7. If required SaaS solutions are not provided through CDT, Agencies/state entities may acquire other commercial and/or government SaaS solutions.
8. If an Agency/state entity determines that the use of a cloud service solution is not feasible, or the required solution is not provided through CDT, they shall submit an exemption request to CDT for approval. The Cloud Computing Exemption Process is defined in Statewide Information Management Manual (SIMM) 18.
9. Classify the data managed by the applications that utilize cloud service models in accordance with SAM 5305.5.
10. Ensure compliance with the security provisions of the SAM (Chapters 5100 and 5300) and the SIMM (Sections 58C, 58D, 66B, 5305A, 5310A and B, 5325A and B, 5330A, B and C, 5340A, B and C, 5360B).

(Continued)

11. Based on data classification pursuant to SAM 5305.5, ensure compliance with relevant security provisions including those in the California Information Practices Act (Civil Code Section 1798 et seq.), Internal Revenue Service (IRS) Publication 1075, Social Security Administration (SSA) Electronic Information Exchange Security Requirements, Payment Card Industry Data Security Standard (PCI DSS) including the PCI DSS Cloud Computing Guidelines, Health Insurance Portability and Accountability Act (HIPAA) Security Rule, Health Information Technology for Economic and Clinical Health (HITECH) Act, and Criminal Justice Information Services (CJIS) Security Policy.
12. Ensure that the commercial and/or government cloud service provider's Standards for Attestation Engagements No.16 Service Organization Control (SOC) 2 Type II report along with the cloud service provider's plan to correct any negative findings is available to the Agency/state entity.
13. Ensure that all confidential, sensitive or personal information is encrypted in accordance with SAM 5350.1 and SIMM 5305-A, and at the necessary level of encryption for the data classification pursuant to SAM 5305.5.
14. Ensure cloud service agreements include all of the DGS' Cloud Computing Services Special Provisions, and all written agreements with cloud service providers address SAM 5305.8 provisions.
15. Ensure that the physical location of the data center, where the data is stored, is within the continental United States, and remote access to data from outside the continental United States is prohibited unless approved in advance by the State Chief Information Security Officer.
16. Maintain an exit strategy for IT solutions that utilizes a commercial and/or government cloud service. The exit strategy must include the Agency's/state entity's ability to export data in pre-defined formats and maintain, when needed, a current backup of the data in the Agency/state entity's designated Tier III-equivalent data center facility. Designated data center facilities must be unrelated to the cloud provider; data center assignments are described in SAM 4982.1
17. Maintain an effective incident response and mitigation capability for security and privacy incidents in accordance with SAM 5340. Report suspected and actual security incidents in accordance with the criteria and procedures set forth in SIMM 5340-A and other applicable laws and regulations.

OPEN SOURCE AND CODE REUSE POLICY INTRODUCTION 4984

(New 05/2018)

The California Department of Technology (CDT) is committed to improving the way Agencies/state entities buy, build and deliver information technology (IT) and software solutions to better support cost efficiency, effectiveness, and public experience with government programs. Enhanced reuse of custom-developed code across state government can have significant benefits for taxpayers, including decreasing duplicative costs for the same code.

To maintain previous investment(s) in IT software, Agencies/state entities shall make code custom-developed by the State of California broadly available for reuse across state government in a consistent manner. This policy is intended to avoid duplicative custom software investments and promote innovation and collaboration across state government while adequately addressing relevant statutory and policy requirements associated with State IT systems, including information security and risk management, privacy, legal issues, and other applicable requirements. The requirements outlined in this section apply to source code that is custom-developed by the State of California, subject to the limited exceptions outlined in SAM Section 4819.2.

OPEN SOURCE AND CODE REUSE POLICY REQUIREMENTS 4984.1

(New 05/2018)

As part of the Open Source and Code Reuse policy, each Agency/state entity shall:

1. Evaluate, as part of the Project Approval Lifecycle alternatives analysis, existing state software solutions for all reportable and non-reportable IT projects. Alternatives analysis shall give preference to the use of existing state software solutions.

2. If alternatives analysis concludes that existing state software solutions cannot efficiently and effectively meet the needs of the Agency/state entity, the Agency/state entity must explore whether its requirements can be satisfied with an appropriate commercially-available solution or open source solution.

3. Use best practices to ensure custom-developed code, documentation, and other associated materials are delivered from developers throughout the software development lifecycle.

4. Create and maintain an enterprise code inventory that includes all new State of California custom-developed code and related information and make this information available to all other Agencies/state entities on an ongoing basis. See code.ca.gov for additional information.

5. Make custom-developed code broadly available for reuse across state government and make their code inventories discoverable through code.ca.gov, the California Department of Technology's code repository, pursuant to the limited exceptions outlined in SAM Section 4984.2.

6. Maintain and frequently update all custom-developed code available in the code repository to ensure code integrity.

7. Whenever possible, secure the rights necessary to make code custom-developed by the State of California available to the public as OSS, pursuant to the limited exceptions outlined in SAM Section 4984.2. Each Agency/state entity's Chief Information Officer (CIO), with consultation from the Agency/state entity's Information Security Officer (ISO), is responsible for determining if the Agency/state entity's custom-developed code will be shared with the public as Open Source Software (OSS) and controlling public access through the Department of Technology's code repository. Agency/state entities must attribute Copyleft licenses (e.g. GPL v.3) to all custom-developed code made OSS to prohibit the creation of proprietary derivative software.

OPEN SOURCE AND CODE REUSE EXCEPTIONS 4984.2

(New 05/2018)

Nothing in SAM Section 4984 shall be construed to require Agencies/state entities to make custom developed-code available as Open Source, if, on the facts of the particular case, disclosure of that code would reveal vulnerabilities to, or otherwise increase the potential for an attack on, an information technology system of an Agency/state entity. The exceptions provided below may be applied, in specific instances, to exempt an Agency/state entity from sharing custom-developed code with other Agencies/state entities. Any exceptions used must be approved and documented in the enterprise code inventory by the Agency/state entity's Chief Information Officer (CIO) for the purposes of ensuring effective oversight and management of information technology resources.

Applicable exceptions are as follows:

1. The sharing of the source code is restricted by law or regulation, including—but not limited to—patent or intellectual property law, the Export Asset Regulations, the International Traffic in Arms Regulation, and the Federal laws and regulations governing classified information;

2. The sharing of the source code would create an identifiable risk to the detriment of national security, confidentiality of Government information, or individual privacy;

3. The sharing of the source code would create an identifiable risk to the stability, security, or integrity of the Agency/state entity's systems or personnel;

4. The sharing of the source code would create an identifiable risk to the Agency/state entity's mission, programs, or operations.

DESKTOP AND MOBILE COMPUTING POLICY 4989

(Revised 02/2017)

The California Department of Technology (Department of Technology) delegates authority to acquire desktop and mobile computing commodities to Agencies/state entities that have submitted acceptable Technology Recovery Plans or Technology Recovery Plan certifications, maintain compliance with all applicable state IT security provisions as defined in SAM Sections 5300-5399, and have appropriate plans for the use of desktop and mobile computing commodities.

Under the Desktop and Mobile Computing Policy, Agencies/state entities are delegated the authority to acquire desktop and mobile computing commodities to support increased staffing, as well as the ongoing replacement of obsolete or nonfunctioning desktop and mobile computing commodities.All acquisitions related to desktop and mobile computing must be consistent with the Agency/state entity's overall strategy for the use of information technology, as expressed in its current Agency Information Management Strategy (AIMS) (See SAM Sections 4900.2 - 4900.6). Agencies/state entities must ensure that the use of mobile computing devices will cost-effectively meet a significant business need and increase the efficiency of the Agency/state entity.

Many desktop and mobile computing commodities are targeted to consumers rather than business users. While these consumer-based commodities are effective as consumer devices, they may not be well-suited for many business uses. To ensure commodities support business productivity and enterprise capabilities, Agency/state entities must understand their security and architecture requirements and acquire the right tools to meet those requirements. Desktop and mobile computing configurations must make use of proven, "off-the-shelf" hardware and software and must support business productivity and enterprise capabilities such as:

- Enterprise Productivity (MS Office)
- Access to Corporate Servers (File/Print, Active Directory, etc.)
- Enterprise Class Applications (Geographic Information Systems, Enterprise Resource Planning, etc.)
- Enterprise Security (VPN, Active Directory Authentication, Multifactor Authentication, etc.)

The acquisition of new mobile computing devices for existing staff should replace existing desktop computers or mobile computing devices, not be purchased in addition to a desktop computer (for example a new laptop should replace a desktop computer). Additionally, the acquisition of new mobile phones should replace desk phones when practical. Replacement of desktop and mobile computing commodities acquired as part of a previously approved IT project, as defined in SAM Section 4819.2, may be included in this policy as such commodities are incorporated into and are no longer distinguishable from the Agency/state entity's IT infrastructure.

DEFINITION OF DESKTOP AND MOBILE COMPUTING **4989.1**
(Revised 02/2017)

Communication – For the purpose of interpreting this policy, communication is the requesting, sending, transmitting, or receiving of electronic data via cable, telephone wire, wireless, or other communication facility.

Desktop and Mobile Computer Software – Commercially licensed software necessary for the operation, use, and/or security of desktop and mobile computers.

Desktop and Mobile Computer Supplies – Consumable commodities used for data storage, printing, and/or other IT supplies as defined in SAM Section 4819.2.

Desktop and Mobile Computing – For the purposes of this policy, desktop and mobile computing is the use of desktop and mobile computing commodities in support of state Agency/state entity business operations.

Desktop and Mobile Computing Commodities – Hardware and software commonly required for most state employees to perform daily business transactions such as desktop computers, mobile computers (e.g., personal digital assistants, laptop computers), mobile phones (e.g. cell phones, smartphones), desktop and mobile computer software, servers, server software, peripheral devices (e.g., printers), supplies, and Local Area Network infrastructure.

Desktop and Mobile Computing Servers – Computer servers necessary for the operation, use, and/or security of desktop and mobile computers.

Desktop and Mobile Server Software – Commercially licensed server software necessary for the operation, use, and/or security of desktop and mobile computers.

Desktop Computers – Computing devices, generally designed to remain in a fixed location, that can connect by cable, telephone wire, wireless transmission, or via any Internet connection to an Agency/state entity's IT infrastructure and/or data systems.

Information Technology Asset Management – The effective tracking and managing of IT assets for an Agency/state entity's program and enterprise IT infrastructure and production systems, including the ability to identify and classify Agency/state entity-owned hardware and software, telecommunications, maintenance costs and expenditures, support requirements (e.g., state staff, vendor support), and the ongoing refresh activities necessary to maintain the Agency/state entity's IT assets.

(Continued)

(Continued)
DEFINITION OF DESKTOP AND MOBILE COMPUTING **4989.1** (Cont. 1)
(Revised 6/2015)

Information Technology Infrastructure – An Agency/state entity's platform for the delivery of information to support Agency/state entity programs and management. Included in the infrastructure are equipment, software, communications, rules, and vision.
Local Area Network (LAN) – Two or more desktop or mobile computers at the same site connected by cable, telephone wire, wireless or other communication facility providing the ability to communicate or to access shared data storage, printers, or other desktop and mobile computing commodities.
Mobile Computers – Portable-computing devices that can connect by cable, telephone wire, wireless transmission, or via any Internet connection to an Agency/state entity's IT infrastructure and/or data systems. The following devices are considered mobile computers:

Laptop/Notebook – A portable Personal Computer (PC) with a clamshell form factor that combines many desktop computer external components into a single device, such as display, speakers, keyboard, and pointing devices. These devices typically run standard PC operating systems. Laptop/Notebook category includes several variations and form factors which include the following:

-Clamshell - traditional laptop/notebook form factor. All the same attributes/components of a PC, but with the keyboard and monitor attached, and of a size that enables for mobile use.

-Ultrabook - laptops that are <u>thinner</u> with <u>longer battery life</u> and <u>touchscreen</u>, <u>wireless display</u>. The Ultrabook category includes 2-in-1 devices that have the ability to convert their look and feel from a traditional clamshell laptop to a tablet/slate. The conversion can be accomplished by detaching, sliding, folding, twisting, etc.

Tablet/Slate– A one-piece mobile computer usually equipped with a touchscreen and an on-screen, hide-able virtual keyboard. Touch is the primary user interface for a tablet/slate device. These devices are typically larger than smartphones and generally have larger screen size and greater computing capabilities. Tablet/Slate devices often have device-specific operating systems such as Apple IOS, Android, or Windows RT.

(Continued)

(Continued)
DEFINITION OF DESKTOP AND MOBILE COMPUTING **4989.1** (Cont. 2)
(Revised 02/2017)

Remote Access – The connection of an information asset from an off-site location to an information asset on state IT infrastructure.

Mobile Phone – A device that can make and receive telephone calls over a cellular network. Mobile phones include smartphone devices which are computing devices that provide advanced computing capability and connectivity, and run a complete operating system and platform for application developers and users to install and run more advanced applications.

Wide Area Network (WAN) – Two or more physical locations connected by cable, wire, or other wireless transmission, providing the ability to communicate between locations and/or Internet connectivity.

EXCLUSIONS **4989.2**
(Revised 02/2017)

The following activities require prior approval from the Department of Technology and are excluded from the delegation authority to acquire desktop and mobile computing commodities. These activities must be treated in accordance with SAM Sections 4819.3 through 4819.42**.**

IT Projects – As defined in SAM Section 4819.2, beyond the acquisition, installation, and operation of **Desktop and Mobile Computing Policy** commodities as defined in this policy. The acquisition of desktop and mobile computing commodities required for an IT project, whether reportable or delegated, must be included within the project scope and acquired under the approved project's authority. Use of this policy to circumvent IT project reporting requirements or to make an otherwise reportable project fall within delegated thresholds is expressly prohibited.

Budget Actions – Any acquisition, maintenance, or support of desktop and mobile computing commodities which requires a Budget Change Proposal, a Budget Revision, or other budget action is not covered by the Desktop and Mobile Computing Policy. However, this policy may be used to acquire the standard complement of desktop and mobile computing commodities as approved by the Department of Finance for new positions.

Specialized or Single-Purpose Systems – Acquiring any specialized, single-purpose, non-modifiable system, such as computer-aided design systems, desktop publishing systems, programmer workbench systems, or artificial intelligence systems is excluded from the policy. However, software-based applications used on a general-purpose personal computer may be covered by the policy. For example, desktop publishing employing word processing, graphics, and page layout software packages on a general-purpose personal computer falls within this policy; desktop publishing employing a specialized computer system that has been developed and marketed for the sole purpose of doing desktop publishing does not. A specialized, single-purpose system that allows some connectivity to an Agency/state entity's existing systems, such as electronic mail, is still considered a specialized or single-purpose system for the purposes of this policy.

(Continued)

(Continued)
EXCLUSIONS **4989.2** (Cont. 1)
(Revised 02/2017)

Infrastructure or Platform Migration – Acquisitions associated with or mandated by a change in an Agency/state entity's standard technical architecture for servers, desktops and/or mobile computing platforms are excluded from the policy. Migrating to a newer version within the existing standard's product family is not considered an infrastructure or platform migration.

Wide Area Networks (WAN) – The acquisition, maintenance, or support of desktop and mobile computing commodities specifically to install or operate a WAN are excluded from the policy. These activities for WANs are considered IT projects, or components of IT projects, for the purposes of this policy. However, upgrading the capacity of a previously approved WAN project may fall within the definition of a previously approved project. (See SAM Section 4819.2: "Previously Approved Effort/Project".)

While the acquisition of desktop and mobile computing commodities specifically for or required by the above-mentioned activities is specifically prohibited under this policy, existing desktop and mobile computing commodities purchased under this policy may be used for some of these purposes. For example, existing desktop computers purchased under this policy may be used in the development of a reportable IT project. Whenever an Agency/state entity is uncertain as to whether a proposed use of desktop and mobile computing commodities falls within the scope of this policy, it should seek a determination from the California Department of Technology.

AGENCY/STATE ENTITY ROLES AND RESPONSIBILITIES **4989.3**
(Revised 02/2017)

Management. Day-to-day management responsibility for desktop and mobile computing configurations resides with the manager who has supervisory responsibility for the individual or individuals who use the products. The manager must ensure that the acquisition and use of desktop and mobile computing commodities support the accomplishment of Agency/state entity objectives and that the individual or individuals who will be using the products are trained in their use.

Each Agency/state entity must have a plan for the appropriate application of desktop and mobile computing. Each Agency/state entity must ensure that its plans are consistent with the Agency/state entity's information management standards, policies, and procedures and its IT infrastructure. Agency/state entity plans for implementing desktop and mobile computing must not preclude the implementation of other Agency/state entity's applications on the same configuration. Agencies/state entities are responsible for establishing desktop and mobile computing standard configurations, ensuring each acquisition made under this policy is consistent with those standards, and accurately tracking the costs associated with such acquisitions. In addition, Agencies/state entities are responsible for the creation and maintenance of IT assets inventories for commodities purchased under this policy.

Agency/state entity's management has a responsibility to establish standards of technical assistance in support of Local Area Network activities such as installation, configuration, problem-determination, maintenance, backup, recovery, and required activities beyond those normally associated with stand-alone desktop or mobile computers. Agencies/state entities are expected to maintain internal processes to ensure that any IT commodities acquired under the authority of this policy are compliant with all applicable hardware, software, and security standards for the Agency/state entity.

Agency/state entity management is responsible for taking appropriate action in the event of employee misuse of desktop and mobile computing technology or employee failure to comply with State and Agency/state entity policy governing the use of desktop and mobile computing.

(Continued)

(Continued)
AGENCY/STATE ENTITY ROLES AND RESPONSIBILITIES **4989.3** (Cont. 1)
(Revised 02/2017)

Security. Desktop and mobile computing environments owned by Agencies/state entities involve the risk of property loss, threats to privacy, and threats to the integrity of state operations. Accordingly, Agencies/state entities must be in compliance with all applicable provisions of the SAM and must implement appropriate safeguards to secure the Agency/state entity's desktop and mobile computing infrastructure.
Use of personally owned smartphones is restricted to devices that are compatible with the CA.Mail or the California Email Service, and are consistent with the Statewide Enterprise Architecture.

Current Agency/state entity Technology Recovery Plans or acceptable Technology Recovery Plan certifications must be on file at the Department of Technology. Agencies/state entities that do not demonstrate effective compliance with the State's IT security policy and Business Continuity policy are not authorized to make any expenditures for desktop or mobile computing commodities until the Agency/state entity has complied. See SAM Sections 5300-5399.

Desktop and Mobile Computing Coordinator. In order to ensure ongoing IT asset management practices are followed, Agencies/state entities employing desktop and mobile computing should designate a unit or individual employee of the Agency/state entity as the Agency/state entity's Desktop and Mobile Computing Coordinator or equivalent function. The coordinator must be knowledgeable about (a) desktop and mobile computing configurations; (b) state-level and Agency/state entity policies for the use of desktop and mobile computing commodities; and (c) the relationship between desktop and mobile computing and other uses of IT within the Agency/state entity.
(Continued)

(Continued)
AGENCY/STATE ENTITY ROLES AND RESPONSIBILITIES **4989.3** (Cont. 2)
(Revised 02/2017)

The responsibilities of the coordinator should include:

1. Maintaining current specifications for the Agency/state entity's desktop and mobile computing commodity standards;
2. Assisting in the completion and review of any Desktop and Mobile Computing (DMCP) documents if required by the Agency/state entity's policies and procedures;
3. Coordinating the acquisition of desktop and mobile computing commodities;
4. Informing desktop and mobile computing users of available training and technical support capabilities; and
5. Maintaining continuing liaison with Agency/state entity IT management to ensure that: (a) proposed desktop and mobile computing applications are consistent with the Agency/state entity's established information management strategy and IT infrastructure, (b) the use of desktop and mobile computing devices is clearly demonstrated and the devices will cost-effectively meet a significant business need and increase the efficiency of the state entity, and (c) desktop and mobile computing configurations can support the implementation of other Agency/state entity applications.

POLICY COMPLIANCE **4989.8**
(Revised 6/2015)

If the Department of Technology determines that an Agency/state entity's procedures or practices are not consistent with the Desktop and Mobile Computing Policy or with the Agency/state entity's own approved policy, delegation of approval authority will be rescinded and the Agency/state entity will be deemed not to have an approved Desktop and Mobile Computing Policy until such time as it can assure the Department of Technology of compliance with an approved policy.