2. California’s Search for Effective IT Governance

The Department of Information Technology (DOIT), which was created in 1995 by the California legislature and began operations in June 1996, was the most recent attempt to organize IT governance at the state level. DOIT, like the preceding organization, emerged as a result of the state’s inability to prevent costly IT project failures. Unlike its predecessor, when DOIT was created, it was set apart from the organization that had historically performed state IT governance. This distinction, and the fact that DOIT’s charter included leadership, guidance, and oversight, led to several problems that plagued the new and unproven DOIT throughout its existence.

The Present Situation

California relies heavily on IT to execute the mission and services of the state. For example:

- Nearly all Department of Transportation (Caltrans) projects involve IT. Computers, networks, and sensors are critical in many areas such as: meters that monitor and synchronize freeway on/off ramps; bridge controls for pumps, ventilation systems, and drainage and traffic flow control systems.
- IT is a large part of the business objective for the Employment Development Department (EDD). EDD currently has initiatives to move into e-government for on-line filing of taxes. The impact of 9/11 on unemployment insurance has resulted in the need for many changes, to accommodate the increased volume for which the system was not originally designed.
- The Board of Equalization’s (BOE) considers IT as the core of its business function rather than an administrative or service function solely.

The ability of these organizations to manage resources and deliver services to citizens is inextricably linked to an expectation of increased effectiveness and efficiency resulting from IT. IT is the heart of delivering many services in the state, and in an Executive Order dated July 1, 2002 (D-59-02), the governor states “information technology is an indispensable tool of modern government.”
The former DOIT was chartered to provide leadership, guidance, and oversight of information technology in the state government. To achieve this mission, it was necessary for DOIT to interact and coordinate with the Department of Finance (DOF) and the Department of General Services (DGS) for control of the process. Likewise, it was necessary for DOIT to interact with the clients of this process, varied agencies and departments, to exchange information that enabled the control decisions and oversight strategies employed by this process. However, the governance under these arrangements suffered many challenges such as the lack of a strategic plan to guide IT project planning and approval, dual project approval authorities, and cumbersome oversight requirements. These contributed to a perception of ineffectiveness on the part of DOIT, which, when combined with highly public and adverse state IT contract negotiations, resulted in a lack of legislative support for the continued existence of the organization.

Thus, although the legislature had previously asked for a review of DOIT’s practices aimed at identifying desirable reforms, it did not intervene to prevent a sunset clause from ending the agency’s existence on July 1, 2002. At that point the governor gave back to departments and agencies primary responsibility for their IT activities. It also gave the Department of Finance (DOF) through its Technology and Investment Review Unit (TIRU) and its Technology Oversight Review Unit (TOSU) technical approval roles for state IT projects. DOF is currently developing and implementing an oversight framework, assessing the current management and oversight practices of departments, agencies, and industry to establish statewide best practices in this area, and handling other aspects of IT issues as they arise (Finance, 2002). DOF is also working on developing a security policy program, capitalizing on the knowledge and assets of state departments to form a security policy advisory group to establish new policies and procedures for IT security. Both the oversight and security plans will continue to develop over the coming months, with periodic updates published in budget and management memorandums.

An Advisor on Information Technology and Chief Information Officer (CIO) for the State of California was appointed on September 20, 2002. The purpose of the new “Advisor/CIO” position is to provide leadership on IT policy and collaborate with other IT leaders in state government. This action was taken in response to the closure of DOIT and the departure of the previous state CIO in June 2002. The current Advisor/CIO reports to the governor but does not have oversight or control responsibilities for state IT initiatives. In this report we do not assess present arrangements for IT governance. Rather, data collected about
California’s governance structures and processes are bounded by the time period of DOIT’s existence.

In what follows, we first describe the establishment of DOIT within the state’s government structure. Then we examine the processes this new entity was intended to carry out. Two appendices supplement this discussion. Appendix B provides a list of the California organizations interviewed and summarizes key comments about DOIT’s procedures and its management capabilities. Appendix C outlines recommendations for performance improvements made to DOIT in spring 2001 and gives indicators of the extent of progress made on each by the time of DOIT’s closure a year later.

The Establishment of DOIT Within State Government

Both size and diversity are key factors that complicate the task of IT governance in the state of California. While other states may face similar challenges and opportunities, California is very different from other states in one key dimension. With 34.5 million residents, it ranks first in population, outnumbering the next biggest state, Texas, by approximately 13 million (U.S. Census Bureau, 2001). These residents are served by a complex architecture of agencies, departments, boards, and other organizational constructs that execute the mission of the state.¹ As noted earlier, the ability of these agencies to deliver mission-critical services increasingly depends on advanced IT. However, by the mid-1990s it was clear that California was not developing the kinds of governance structures and processes that would promote effective IT deployment.

DOIT was created in response to a number of costly and embarrassing problems with implementing various IT projects in California state agencies. The culmination of these failures was documented in three separate reports in 1994 which all found that there was insufficient statewide planning, coordination and leadership for IT (LAO, 1994; Task Force, 1994; BSA, 1994). In response, the California legislature held a series of hearings and passed legislation forming DOIT as an independent agency, with the state’s Chief Information Officer designated by the governor as its director. (SB 1, Alquist, 1994).

Prior to the creation of DOIT, responsibility for IT oversight belonged to the Office of Information Technology (OIT) in the DOF. OIT was created in 1983 to

¹Later in the text, this condition is referred to as the diversity of agencies and departments in California. The differences are due to varied reporting structures (some to the governor, some to elected boards), funding structures (general fund, special funds, federal dollars), IT staff sizes (ranging from 6 to 1000), and vastly differing missions.
replace the State Office of Information Technology (SOIT), also housed in DOF, with a purpose and mission that eventually would become the blueprint for DOIT. OIT was given the responsibility to develop plans and policies for the application and development of IT in the state, and for oversight of state agency IT projects. However, OIT was sharply criticized for failing adequately to perform these responsibilities after a number of costly IT project failures—most notably, the Department of Motor Vehicles database redevelopment project that cost the state $49 million and did not result in a working system. Audits by the Bureau of State Audits and reviews by the Legislative Analyst’s Office and the Task Force on Government Technology Policy and Procurement regarding the state’s IT programs prompted legislative hearings and the introduction of legislation to create a new department that would provide the badly needed leadership and oversight for the state’s IT program.

In 1994, legislation was introduced to create DOIT. In its original form, the legislation included a provision for a cabinet-level CIO and would have transferred all of the former OIT personnel from DOF, and DGS personnel involved with IT acquisition into the new department, to be called the “Information Services Agency.” It would have also consolidated the administration of the data centers under the new entity. The legislation did not pass in this form because of competing interests, and a revised bill (SB1) was approved by the legislature in October 1995 (Peterson, 2002). Some expressed concern over the modified bill, citing the major problem that key positions and power were retained by the DOF. While SB 1 transferred oversight responsibility to the new DOIT, DOF retained financial authority for IT projects in its newly created Technology Investment and Review Unit (TIRU).

DOIT was charged with “providing leadership, guidance, and oversight of information technology in state government” (SB 1, Alquist, 1994). Most of its responsibilities centered on developing plans and policies to support the effective use of IT. This included responsibilities to manage the acquisition and appropriate use of IT in state agencies, to coordinate between various federal, state, and local government stakeholders as well as private industry, and to ensure that agencies’ IT plans and projects were in line with the state’s vision and goals for IT. DOIT was also given direct oversight authority to review, change, or veto agencies’ IT projects as it deemed necessary (SB 1).

Thus, from the very beginning of DOIT’s existence, a number of problems threatened its ability to effectively operate in accordance with legislative intent within the state government structure as it was eventually configured.
DOIT’s Roles in Key IT Deployment Processes

DOIT was initially chartered to provide “leadership, guidance, and oversight” of information technology in state government. Functionally speaking, the IT development processes were conceived in terms of the five steps in Figure 1.

![Figure 1—California’s Information Technology Development Process](SOURCE: “Information Technology: The State Needs to Improve the Leadership and Management of Its Information Technology Efforts,” BSA, June 2001.)

We use this framework below to examine the roles DOIT played in IT development processes.

**Planning**

DOIT’s responsibilities in the planning phase were primarily to collaborate and to advise. One problem DOIT faced was trying to balance this advocacy role with its control function. Another problem was that DOIT never quite established itself as a trusted and credible advisor.

In its collaborative role, DOIT tried to work with departments and agencies when project initiatives were being formed, a step that some thought beneficial to the development and subsequent review of a Feasibility Study Report (FSR).
Effective IT project definition requires consideration of the business objectives, which determine the requirements, and knowledge of and proficiency in the technology. Departments and agencies put significant emphasis on the up-front process to prepare a strong FSR. The nature of this up-front involvement, which DOIT was trying to become more involved in, is quite distinct from the remaining phases of the IT development process. The initial phase is focused on advocacy, while the latter phases focus on control.

In its advisory role, DOIT was supposed to develop a statewide strategic plan, which included revision of the statewide IT plan to address emerging critical IT issues as a result of recent administrative requirements. Subsequently, the statewide strategic plan would guide the development of department/agency IT plans and projects. However, due to California’s size, diversity of department/agency priorities, and complexity of department/agency reporting structures this proved challenging. The process that DOIT used to update the strategic plan was not adequately inclusive of or responsive to department/agency CIOs, and the revision that was drafted, late in DOIT’s existence, was neither well received nor complete. In some cases interviewees were unaware of its existence.

Approval

DOIT’s role and responsibilities relative to other control organizations, in particular for approval, were not well defined or distinguished. SB 1 did not clearly state what roles and responsibilities DOIT would gain and what roles and responsibilities would be retained in DOF (via TIRU). It gave project approval authority to both DOF and DOIT. DOIT, DOF, and to some extent DGS all had a role in the approval process. In principle, DOIT was supposed to review the merits of the technology of a proposed IT project, while DOF would review the business case and approve funding, relying on DOIT’s expertise to inform its decision. In practice, however, DOIT became primarily a “rubber-stamp” department, while DOF made the final decisions about IT project approval (LAO, 1996; interviews, 2002). Client agencies saw DOF and DOIT’s roles as overlapping, even though there was no doubt that the final authority was with DOF. This ambiguity and imbalance of power eroded trust and confidence in these two control agencies from the client perspective.

DOIT’s failure to produce an updated statewide strategic plan may have also contributed to another problem. Clients indicated that the approval process appeared preferential, arbitrary, and unilateral. For example, when a mission-critical prison IT system was denied by DOF, appeals to the administration
overturned this decision because the outcome of not approving the system would have created unacceptable conditions in the prisons. The existence of a strategic plan may alleviate the problem of effectively disapproving (approve but not fund) or inadequately funding projects without consideration of multiyear effects, prior investment of resources, or overall mission objectives. This problem stems not only from a lack of direction that a strategic plan may provide, but also the apparent ability of DOF to exercise line item control (independently make specific cuts in funding or staff) over projects. The statewide strategic plan (and related supporting plans) might have alleviated some ambiguity from approval process by serving as a guide to assess and judge projects. Frustration with the approval (and budgeting) process has motivated some clients to limit exposure to control phases of the IT development processes because they have become increasingly arduous and mired in mistrust.

**Procurement**

Of all the IT development process phases, DOIT’s role in the procurement phase was the least prominent. However, DOIT was beginning to take on the task of leveraging the state’s buying power (a task that many consider appropriate for a statewide entity), but in one particular incident this was not well executed. Legislative hearings accused DOIT of failing to review and assess the needs for a proposed statewide contract with the Oracle Corporation, which if executed, would have resulted in costly and unnecessary purchases of database software licenses for the state. As a result, for a brief period of time the California Multiple Award Schedule (CMAS), Master Service Agreements (MSAs), and Enterprise License Agreements (ELAs)—all vehicles to facilitate procurement and gain economies of scale for the state—were restricted, forcing more competitive bids and unraveling the state’s buying power. Managing the tension between statewide efforts for cost efficiency and effectiveness versus competitive procurements for equity and public trust was and will continue to be a significant challenge.

A related problem that DOIT faced was the definition and use of standards. Most agree that standards are needed and DOIT made some attempts to establish standards, but budgetary concerns regarding the cost impact on projects derailed such endeavors. Even had this not been the case, vendor lobbyists, who wield

---

2 In response to this claim, Finance noted, “If we cut things we expect you to do a different project or justify the project.”

3 New guidelines for the use of these vehicles were issued by the Department of General Services in December 2002.
significant political power, may feel threatened and locked out of competition if standards (other than theirs) are set. DOIT’s inability to make progress in this area contributed to a perception, by some, of ineffectiveness.

Implementation and Evaluation

DOIT’s main role during these phases was oversight: reviewing project progress, assessing the resultant system, and when necessary redirecting or terminating a project. Highly publicized failures with political implications have evolved and expanded the oversight process with the objective of preventing the next troublesome project. As previously stated, DOIT was created with the explicit intent of providing leadership and guidance, as well as conducting oversight (a task that its predecessor allegedly did not satisfactorily perform).

Project oversight occurs at many levels both internal and external to departments/agencies, but there are varied opinions as to how much is necessary and where it should occur. DOIT initiated several strategies to fulfill its oversight responsibilities including the use of Independent Project Oversight Consultant (IPOC) and Independent Verification and Validation (IV&V) contractors. These extra personnel were usually at the expense of the department/agency because DOIT did not have the resources to undertake such an enormous task. The burden of meeting DOIT’s oversight requirements was considered by some excessive, redundant, and at times trivial. In particular some felt that DOIT’s oversight requirement for a department/agency should have been tied to the capability of the organization. On the other hand, some felt that independent oversight was an absolute must, because departments/agencies cannot effectively police themselves.

When asked, interviewees could not recall a specific incident where DOIT actually exercised its authority to terminate a project, possibly due to lack of influence or political support. Some interviewees suggested that DOIT did not have the real authority for oversight of projects, as requested by the Legislature (LAO, 1997).

A key challenge with DOIT’s oversight role (and potentially any entity taking on this responsibility) is the definition of failure. When should a project be considered a failure? The operating definition is some predefined variance from the baseline in budget or schedule. Evidence from other domains suggests that this variance should be anticipated, partly because users are unable to fully
anticipate or appreciate the impact of a new technology on their task or mission. Additionally, other factors beyond the actual implementation of the project may contribute to these changes such as: control portions of the IT development process, the level of collaboration among stakeholders when the IT project spans organizational boundaries, and the dynamics of the state and its needs. Finally, the definition of “failed” may be misleading because failed projects often end up as useful systems. In California’s context, “failed” projects include those that have generated adverse public headlines.

Other Problem Areas

Aside from the problems DOIT encountered with the IT development process, DOIT also faced a series of other problems related to the environment in which it operated. These problems originate from DOIT’s structure and relationships with other organizations, as well as ambiguity in its role and function.

Organization and Support

California interviewees noted that in general SOIT, OIT, and DOIT all had similar constructs and similar challenges—namely, collaboration with and from other stakeholders in the process. Among the control organizations and client departments alike, a collaborative and supportive environment was at times lacking. As an example, interviewees cite DOF’s reluctance to support DOIT’s proposal for IV&V vendors, severely cutting the forecasted amount of contractor support needed for oversight.

According to the LAO, DOIT had neither the active support of the governor’s office nor an adequate number of staff to carry out all the responsibilities it was given (LAO, 1999). DOIT was disadvantaged from the beginning, because none of the staff from the former OIT were permitted to transfer to the new department as it was established. DOIT thus lacked the institutional knowledge, particularly for control, from which to draw upon in carrying out its numerous responsibilities.

\[\text{In military information systems, studies suggest that early/static estimates for systems are often wrong. Specifically, it is “a faulty assumption . . . that users know what their requirements are, or at least should know. In fact, it is unreasonable to expect users to know, in any detail, what their requirements are or will be, when they do not have a full appreciation of the new or improved technologies, particularly in terms of implications for the environment or mission.” Network Centric Warfare, http://www.dodccrp.org/Publications/pdf/ ncw_2nd.pdf.}\]
**Roles and Functions**

DOIT received intermittent support from the governor. Two highly successful initiatives—the Year 2000 conversion effort and the My California Web Portal project—enjoyed the public backing of the governor, but IT initiatives in general received little attention from the administration (Little Hoover Commission, 2000). DOIT received high praise for its role in the California Year 2000 conversion effort. It was credited with providing strong leadership and identifying and acting on problems early, in collaboration with state agencies. On the other hand, DOIT was minimally involved in the My California Web Portal project, and this dispersion of IT responsibilities was seen by some as a lack of confidence in DOIT’s ability.

However, DOIT’s presence as a statewide IT organization may have created inconsistent and unrealistic expectations. California interviewees identified several roles they thought appropriate for a statewide entity. These included items such as responsibility for ubiquitous functions, responsibility to advance initiatives from an enterprise-wide perspective and the provision of a community forum to address common issues. DOIT attempted to do all of these. It tried to set policy and standards for security, it tried to conduct enterprise licensing, and it tried to establish a community forum (CIO meetings) for sharing. All of these were less than successful, possibly because DOIT attempted to tackle too many challenges at once, rather than establish a set of priorities and tackle only the most important issues and challenges, as time and resources permitted.

Lastly, the manner in which DOIT approached these challenges did not always (from the client perspective) seem very collaborative. CIOs felt that DOIT did not consider or listen to what the departments and agencies needed in terms of standards and best practices. Rather, they felt that DOIT mandated many requirements and issued policy without using appropriate feedback and involvement of the clients. In its relationships with both control and client organizations, DOIT sometimes found itself at odds with other IT stakeholders.

**Still Searching for an Answer**

There still exists an unsatisfied need for IT governance in California. DOIT and previous governance structures (OIT, SOIT) fell out of favor when they unsuccessfully negotiated public and politically damaging IT development initiatives. Yet after several organizational attempts to structure IT governance and numerous studies on the challenges of governing IT in California, the state is still searching for an answer on how to govern IT. Given that IT is a core
component of effective government and IT is recognized as critically important, why has IT governance been so problematic? It is instructive to review the conditions under which governance is attempted.

The application of IT in California is significant; it permeates nearly all aspects of state government. It is multifaceted, supporting a multitude of missions, and it is evolving in response to new and on-going needs. The stakeholders include Californians at the individual citizen level as well as private and public sector organizations. It encompasses individual citizens expecting a public good or service from the state and industries seeking business-friendly opportunities via efficient interaction in and with the state. It includes public institutions empowered to provide services for the public good, as well as the executive leadership of the state who are responsible for making decisions that will enhance and improve the state, where possible through the use of IT.

It is highly plausible that under the previously employed governance model, DOIT was neither appropriately defined nor adequately structured to account for the complexity of this task. Like its predecessors, it emerged in response to a perceived failure of the system to protect the investment of the state in IT. Unlike its predecessor, it reported to the governor’s office, instead of an administrative department, and was headed by a state-level CIO. If the governance model is important, what other models are appropriate and would they work given California’s situation? If the solution is greater than the governance model, what other factors contribute to successful IT governance? It is questions such as these that this present study was meant to address.

The following chapter describes our search for alternative models for state IT governance. Our research methods included criteria for selecting the other states whose governance structures we examined; development of a protocol to conduct interviews within those states; and a between-case analysis of the resulting data to generate three general models of IT governance.