California Department of Technology

Weaknesses in Strategic Planning, Information Security, and Project Oversight Limit the State's Management of Information Technology

April 2023

REPORT 2022-114

CALIFORNIA STATE AUDITOR
621 Capitol Mall, Suite 1200 | Sacramento | CA | 95814

916.445.0255 | TTY **916.445.0033**

For complaints of state employee misconduct,
contact us through the **Whistleblower Hotline**:
1.800.952.5665

Don't want to miss any of our reports? Subscribe to our email list at **auditor.ca.gov**

For questions regarding the contents of this report, please contact our Public Affairs Office *at* 916.445.0255

Grant Parks *State Auditor*

April 20, 2023
2022-114

The Governor of California
President pro Tempore of the Senate
Speaker of the Assembly
State Capitol
Sacramento, California 95814

Dear Governor and Legislative Leaders:

As directed by the Joint Legislative Audit Committee, my office conducted an audit of the California Department of Technology's (CDT) oversight of information technology (IT) projects and the State's safeguards against cybersecurity threats. In general, we determined that CDT's weaknesses in strategic planning, information security, and project oversight limit the State's management of IT.

CDT has broad responsibility and authority over nearly all aspects of IT in the State, including providing strategic direction, assessing IT security, and performing project oversight. However, it has not fulfilled important responsibilities in these areas, resulting in significant consequences for the State. CDT has not provided the State with sufficient strategic direction to ensure that critical IT systems are modernized, secure, and that the systems effectively provide important services. For example, CDT has yet to identify the systems statewide that are outdated or obsolete and require modernization, leaving the State at risk of outage or failure.

Additionally, CDT has yet to determine the effectiveness of the State's information security programs and whether the State's IT systems incorporate adequate protection from cyberattacks that could compromise individuals' personal information, shut down critical government functions, and cost the State millions of dollars to remedy. Despite CDT's identifying significant problems in the IT projects it oversees, it has not used its authority to make sure those problems are resolved, which has led to delays, cost overruns, and systems that do not function as intended.

To ensure IT systems' effectiveness and security, CDT must implement a comprehensive statewide strategic plan that clearly sets priorities for addressing the State's IT needs and demonstrates urgency in preparing for and responding to cybersecurity threats. The Legislature should also act to ensure the effectiveness and independence of the State's IT project oversight.

Respectfully submitted,

GRANT PARKS
California State Auditor

Selected Abbreviations Used in This Report

CDT	California Department of Technology
DMV	Department of Motor Vehicles
EDD	Employment Development Department
IT	information technology
NIST	National Institute of Standards and Technology
PAL	project approval lifecycle

Contents

Summary 1

Introduction 3

Audit Results
CDT Has Not Effectively Guided the State's IT Needs 9

CDT Has Not Taken Critical Steps to Assess Whether Reporting Entities Have Implemented Appropriate Safeguards to Protect Their IT Systems 16

CDT's Approval and Oversight Processes Do Not Adequately Mitigate Risks for Complex IT Projects 23

Conclusions and Recommendations 35

Appendix A — Survey Information 43

Appendix B — Contracts and Amendments of the IT Projects We Reviewed 57

Appendix C — Scope and Methodology 61

Response to the Audit
California Department of Technology 65

California State Auditor's Comments on the Response From the California Department of Technology 69

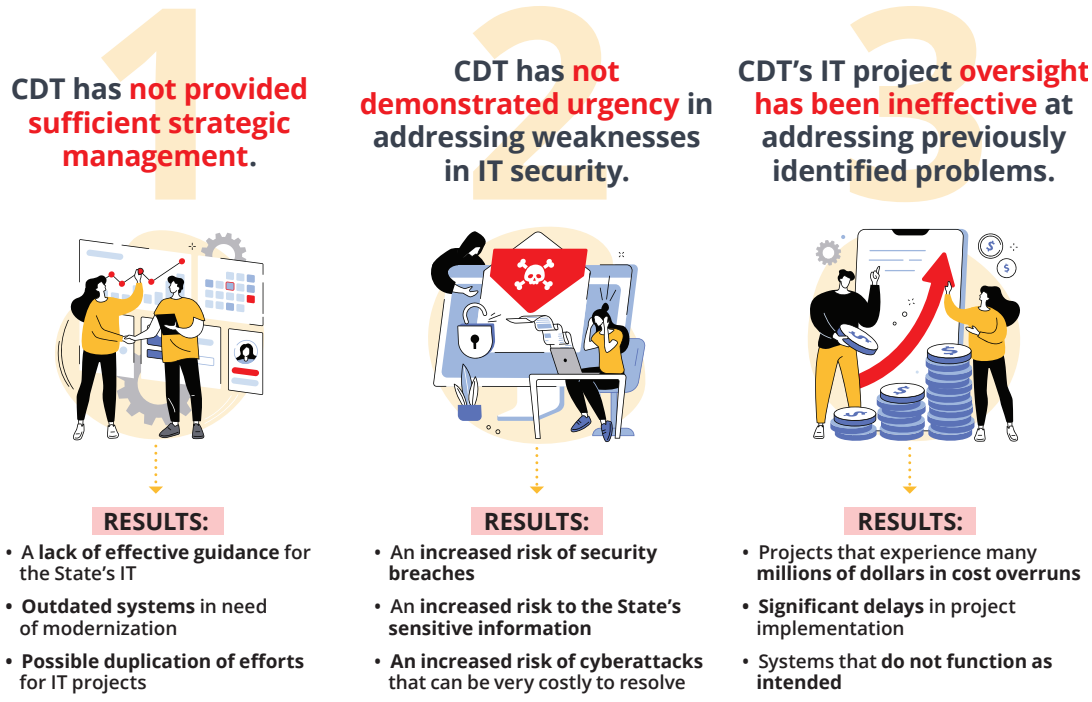
Blank page inserted for reproduction purposes only.

Summary

Results in Brief

The State relies on information technology (IT) to efficiently and reliably provide vital services to millions of Californians. State law and policy give the California Department of Technology (CDT) broad responsibility and authority over all aspects of IT in the State. For example, state law requires that CDT produce a strategic plan to guide the State's IT activities, including efforts to modernize critical systems. CDT's duties also include providing direction for information security to state agencies in the face of the threat of cyberattacks. Moreover, CDT has the responsibility to oversee state agencies' IT projects and the authority to approve, suspend, terminate, and reinstate those projects as necessary. However, as we show in Figure 1, CDT has not fulfilled important responsibilities in the areas of strategic management, IT security, and project oversight, resulting in significant consequences for the State.

Figure 1
CDT's Struggles to Fulfill Critical Responsibilities Have Had Significant Consequences for the State



Source: CDT's strategic plans for 2017 through 2023, project oversight reports, information security compliance audits, interviews with CDT's staff, and our independent IT expert.

Despite its responsibilities under state law, CDT has not followed best practices for strategic planning, hindering the State's ability to determine whether it is meeting its IT goals or whether its efforts related to IT are efficient and effective. Rather, CDT asserted that its IT goals are aspirational and not intended to be a performance

measure for all state agencies. However, because CDT has not provided the State with a clear strategic direction, state agencies have not had a roadmap for prioritizing IT-related needs—such as modernizing critical systems. In fact, CDT has yet to identify the systems statewide that are outdated or obsolete and that require modernization, leaving the State at risk of outage or failure. Further, it has not strategically managed IT systems that have similar functions to enable the efficient use of IT statewide and to avoid duplication of costs and efforts.

Additionally, CDT has not ensured that the State's IT systems are adequately protected from cyberattacks that can compromise individuals' identities, shut down critical government functions, and cost the State millions of dollars to remedy. For example, CDT has stated that to improve the State's information security programs, it must be able to effectively determine the status of information security across the State as a whole and within each state agency individually. However, it has yet to determine the effectiveness of the State's information security programs. Further, in those instances when it has assessed state agencies' information security, those agencies' security statuses have tended to decline subsequently rather than improve. Moreover, CDT has not taken adequate steps to educate state agencies on the cybersecurity threat monitoring service that it provides at no cost.

Lastly, CDT's inadequate oversight of IT projects has been insufficient in preventing delays and has led to tens of millions of dollars in cost overruns and systems that do not fully function as intended. Despite identifying significant problems in the IT projects it oversees, CDT has not used its available authority to ensure that those problems are resolved. According to CDT, its general oversight approach is collaborative, iterative, and incremental. However, it has not suspended or terminated a project since 2016. Further, the project approval process CDT has established does not include critical steps that might identify and address risks during the project planning stage. Improving the State's project oversight is critical given that the State is working on 29 IT projects for 20 different agencies for an estimated total cost of $3.7 billion, as of November 2022.

Over the past 10 years, our multiple audits of CDT have identified the same or similar problems. Nevertheless, CDT has continued to struggle to demonstrate critical aspects of leadership, such as ensuring accountability, setting priorities, demonstrating urgency, and maintaining independence. The Legislature should make changes to ensure the effectiveness and independence of the State's IT project oversight. We describe our recommendations in detail beginning on page 39 and believe they are essential to address weaknesses in the State's management of IT.

Agency Comment

Although CDT disagreed with many of our conclusions, it indicated that it would consider our recommendations.

Introduction

Background

California residents and businesses depend on the State for a variety of important services, as Figure 2 shows. To provide these services, the State relies on information technology (IT). IT systems are vital to nearly every facet of state government; for example, they hold voter registration records, help identify locations for highway construction projects, and manage the finances that keep the State functioning. In the text box, we provide specific examples of other essential services that depend on IT systems. In many ways, IT systems are critical to ensuring that state government functions effectively.

At its best, IT can increase the efficiency of state services and reduce the overall cost of government. At its worst, IT can cause inconvenience, contribute to delays, create security risks, or prevent access to services altogether. Over roughly the past two decades, California has experienced significant challenges related to its IT infrastructure. These challenges include failed IT projects that cost the State hundreds of millions of dollars, system outages that left Californians unable to access critical services, and inefficiencies resulting from outdated technology that likely have resulted in frustration and misgivings about government effectiveness.

Examples of Vital Services That the State Provides Using IT Systems

Medical services: The California Medicaid Management Information System (CA-MMIS) processes about 200 million claims annually for Medi-Cal members' medical services, resulting in more than $19 billion a year in payments to health care providers.

Motor vehicle services: In fiscal year 2020–21, nearly 1.8 million customers renewed their driver's licenses using the Internet, 12.2 million renewed their vehicle registrations using the Internet, and another 2.7 million used the Department of Motor Vehicles' self-service kiosks.

Social services: Individuals can apply online for key public assistance programs such as CalFresh and CalWorks, which are supported by California's Statewide Automated Welfare System (CalSAWS).

Unemployment insurance: Millions of individuals and employers participate in the Unemployment Insurance program in California. Since March 2020, 28 million claims have been filed, and the State has paid $184 billion in benefits. Individuals can apply for unemployment insurance benefits online.

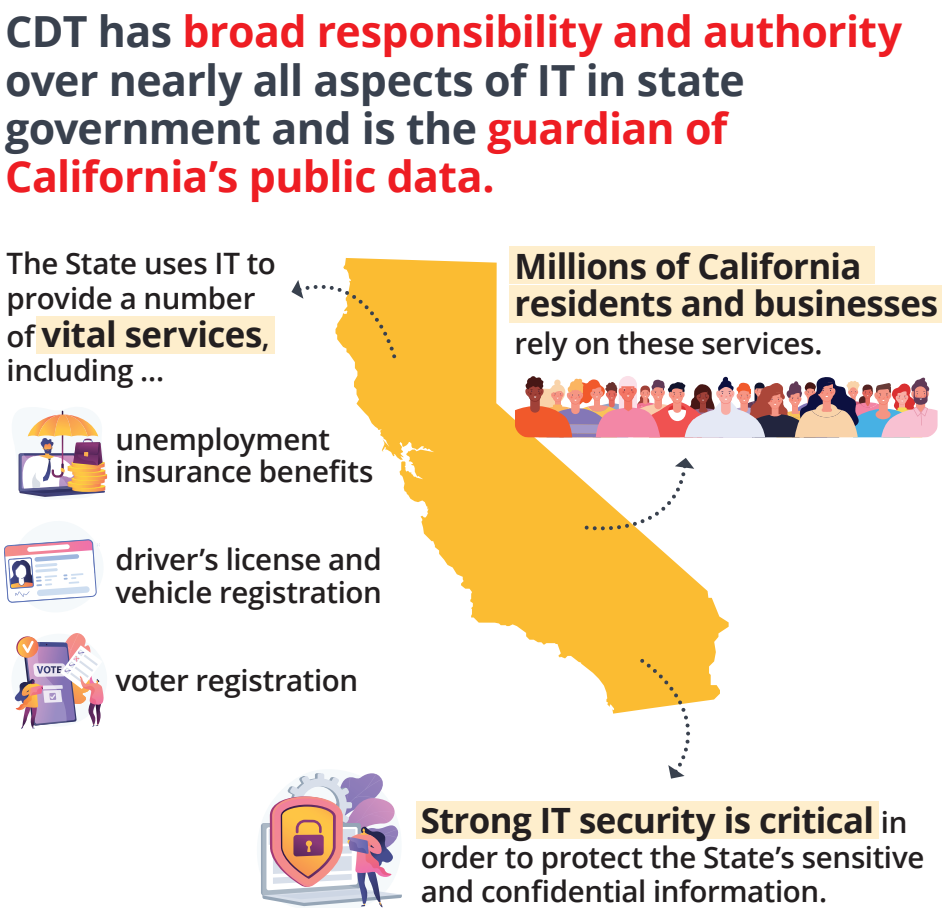
Source: Various system documentation and agency websites.

CDT Has Broad Responsibility for State IT

State law and policy give the California Department of Technology (CDT) responsibility for and broad authority over nearly all aspects of IT in state government. Figure 3 shows that CDT is under the Government Operations Agency in the executive branch and is organized into several offices. CDT has more than 1,000 total staff to perform its responsibilities and a proposed budget of approximately $830 million in the Governor's budget for fiscal year 2023–24. CDT has summarized the scope of its IT responsibilities in its mission statement,

as the text box shows.[1] The text box also includes CDT's statement of its roles and responsibilities, which include guarding public data and leading IT services and solutions. CDT has documented its duties and processes in the *State Administrative Manual*, a reference resource for statewide policies, procedures, and requirements, and in the *Statewide Information Management Manual*, a compilation of standards, instructions, forms, and templates that state agencies must use to comply with IT policy.[2]

Figure 2
The State Relies on IT to Provide Vital Services to Millions of Californians



Source: *State Administrative Manual* and state agencies' websites.

[1] According to CDT's mission, it also partners with local government and educational agencies. However, our audit focused on CDT's role in relation to state agencies.

[2] When referring in general to multiple, or a variety of, California's governmental entities, we use the term "state agencies." According to Government Code section 11000, the term *state agency* encompasses every state office, officer, department, division, board, and commission.

State law specifically tasks CDT with advising the Governor on the strategic management and direction of the State's IT resources. The law states that CDT must produce an annual IT strategic plan to guide the State's acquisition, management, and use of IT; and it directs CDT to take all appropriate and necessary steps to implement that plan. Moreover, state law effective September 2021 requires CDT to identify, assess, and prioritize high-risk, critical IT systems to ensure that they are stable and up to date in order to meet changing state needs. State law also requires CDT to submit an annual report to the Legislature describing how it is prioritizing these efforts.

CDT's Mission Statement

Mission: "The California Department of Technology is committed to partnering with state, local government and educational entities to deliver digital services, develop innovative and responsive solutions for business needs, and provide quality assurance for state government IT projects and services."

Roles, Responsibilities, and Authority: "CDT is the guardian of public data, a leader in IT services and solutions, and has broad responsibility and authority over all aspects of technology in California state government, including policy formation, interagency coordination, IT project oversight, information security, technology service delivery, and advocacy."

Source: CDT's organization guide.

In addition, state law requires CDT to issue and maintain policies, standards, and procedures governing the State's information security. State agencies within the executive branch that are under the Governor's direct authority (reporting entities) are required to comply with these policies and procedures and to report to CDT on their compliance. State law also gives CDT the authority to conduct independent security assessments of every state agency, department, or office.

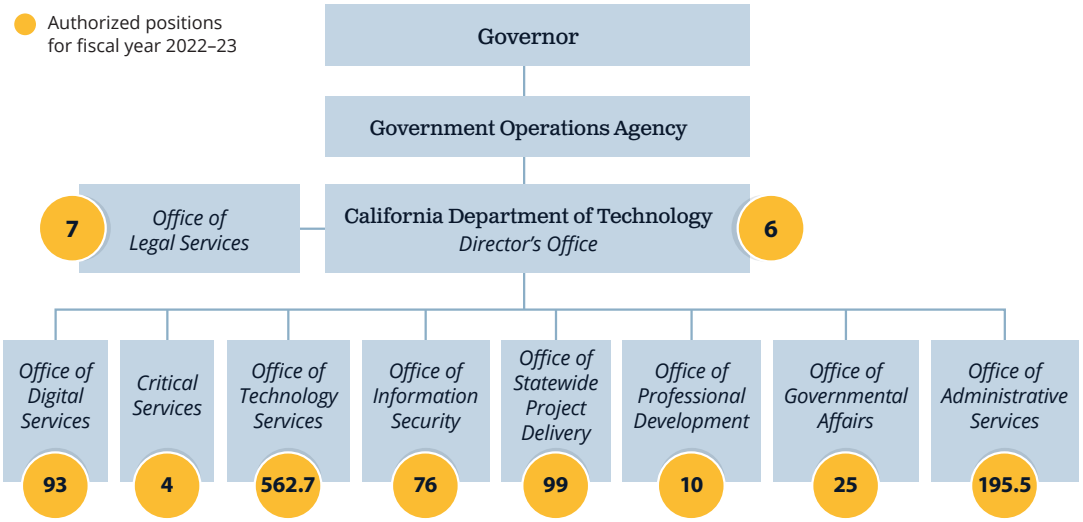
Finally, CDT is responsible for providing oversight of the State's IT projects. It has the authority to approve, suspend, terminate, and reinstate IT projects. State law authorizes CDT to delegate approval and oversight of these projects to agencies. CDT will delegate approval authority to an agency based on an assessment of the agency's project management, project oversight, and performance on previous IT projects. For IT projects that cost $5 million or less, CDT may delegate approval and oversight to state agencies according to cost thresholds (delegated IT project). CDT retains project approval and oversight responsibility for all IT projects that cost more than $5 million or meet certain conditions (nondelegated IT projects), for example, if the project involves a new system development that is specifically required by legislative mandate or CDT and/or the agency information officer has determined that the project has criticality or risk factors that warrant continued approval and oversight by CDT.

CDT Provides Various IT Services to State Agencies

In addition to its leadership and oversight responsibilities, CDT provides a range of IT services to other state agencies—including infrastructure and platform services, network and telecommunications services, software services, professional services, and security services as well as IT support. State agencies also generally have their own staff who take on IT-related responsibilities. These staff include department chief information officers (chief information officers) who are overseen by agency information officers. Agency information officers are responsible for overseeing an agency's IT assets, projects, data systems, infrastructure, and services through their management of the chief information officers within their agency. A chief information

officer is responsible for all IT-related activities within a state agency and for ensuring that the agency conforms to state IT policy. The director of CDT is responsible for providing technology direction to agency information officers and chief information officers to promote the alignment and effective management of IT services.

Figure 3
CDT's Structure Encompasses Several Offices



Source: CDT documentation, California state government organizational chart, and California Department of Finance position data.

We conducted an online survey of state agency information officers and chief information officers to determine which of CDT's services their agencies use and their satisfaction with those services. We sent the survey to 143 state agencies and received 103 responses.[3] Many of the agencies indicated that they use CDT's services that relate to network access, website management, IT procurement, and IT project approval and oversight. Our survey also included questions about IT security, IT systems in need of modernization, and digital services. We have referenced the agencies' responses throughout this report to provide context regarding their perspectives. An aggregated summary of our survey is included in Appendix A.

Other State Agencies Also Provide IT Services

Several other state agencies have IT-related responsibilities. For example, the Department of General Services (General Services) shares IT procurement responsibilities with CDT. Specifically, General Services determines IT procurement procedures for the purchase of certain IT goods and services, such as the ongoing

[3] We include additional information about the survey in Appendix A.

replacement of desktop computers. In another example, the California Military Department works with CDT to perform independent security assessments of state entities. These assessments provide a technical evaluation of an agency's network and selected web applications to identify security vulnerabilities.

The Office of Data and Innovation also has IT-related responsibilities. Its stated mission is to deliver better services to Californians through human-centered design and technology. It focuses on engaging directly with the public and state agencies to identify opportunities for continuous improvement in service delivery and on designing reusable or scalable human-centered solutions related to services. An example of the Office of Data and Innovation's work is the creation of covid19.ca.gov—a COVID-19 informational website. Additionally, the Office of Data and Innovation collaborates with CDT on the California Design System, which is a set of principles, design guides, and components intended to make digital information and services easier to use so that state websites can better serve the public. Although the Office of Data and Innovation's mission differs from CDT's, there are similarities in some of their responsibilities. For instance, CDT's Office of Digital Services provides organizational leadership focused on improving how state government develops and implements innovative technology solutions to meet the public's evolving needs.

Blank page inserted for reproduction purposes only.

Audit Results

CDT Has Not Effectively Guided the State's IT Needs

CDT has not provided the State with sufficient strategic direction to ensure that critical IT systems are modernized and secure and that the systems effectively provide important services. Specifically, CDT has not followed best practices when developing the State's IT strategic plan and is consequently unable to effectively determine whether the State is meeting the plan's goals. In addition, CDT has yet to establish a process to identify and assess IT systems that require modernization. Finally, it has not strategically managed the many state IT systems with similar functions to ensure their efficient use and avoid the duplication of IT-related efforts.

CDT Has Not Followed Best Practices for Strategic Planning

Statewide strategic planning is one of CDT's main statutory responsibilities. Specifically, state law requires the director of CDT to produce an annual IT strategic plan that guides the State's acquisition, management, and use of IT. Such planning is critical because it helps develop commitment to an organization's mission and aligns organizational resources with long-term goals. The *State Administrative Manual* affirms that strategic planning is essential to the successful adoption of IT in state government.

Key Best Practices for Strategic Planning

- Prepare a mission statement.
- Assess environmental factors and critical issues.
- Identify a small number of broad goals.
- Develop measurable objectives that are the specific results intended to be achieved through the strategic plan.
- Monitor progress toward planned goals.

Source: State, federal, and other entities' best practices documentation.

State, federal, and other entities have identified best practices for establishing a sound strategic planning process. The text box lists a number of these practices. Following best practices allows an organization to effectively strategize how to fulfill its mission, know whether it is meeting its goals, and adjust its operations in the event of changing circumstances. Accordingly, we expected CDT to employ these practices to provide the State with strategic direction for ensuring that its critical IT systems are modernized, secure, and technologically effective.

However, CDT did not follow many of these key best practices when developing its two most recent strategic plans. According to CDT, it develops each strategic plan in collaboration with various agency information officers and chief information officers so that the strategic plan represents the collective goals and objectives of the State. CDT developed broad goals for its current strategic plan for 2021 through 2023, as the text box describes. However, as Figure 4 shows, the strategic plan does not include measurable objectives, such as a description of specific tasks or timelines necessary to achieve the broad goals.

CDT's Strategic Goals for 2021 Through 2023

1. Deliver easy-to-use, fast, dependable, and secure public services.
2. Ensure public services are equitable and inclusive.
3. Make common technology easy to access, use, and reuse across government.
4. Build digital government more quickly and more effectively.
5. Build confident, empowered multidisciplinary teams.

Source: CDT's strategic plan *Vision 2023*.

Figure 4
CDT's Poor Strategic Planning Process Has Left the State Without an Effective Plan for Its IT

Source: CDT strategic plan for 2021 through 2023 and analysis of key best practices.

* Although the strategic plan did not include the mission statement, CDT has prepared and documented its mission statement on its website and in other resources.

For example, one of the goals of the current strategic plan is to "deliver easy-to-use, fast, dependable, and secure public services." CDT's strategic plan identifies challenges related to the goal in the form of questions, such as "What must we do to ensure critical public services and IT infrastructure are ready for surges, and are resilient and dependable?" However, the plan does not include objectives to address the challenges it identifies; instead, it leaves the questions unanswered. The plan also does not identify the critical public services to which this goal refers, provide measurable definitions for the ease of use and dependability of such services, or include a timeline for achieving the goal. CDT lacks similar information for its other four current strategic goals. CDT asserted that the goals in its strategic plan are aspirational and that it is difficult to create performance measures for all state agencies. However, an example of a measurable objective for its first goal could be to identify key public services and ways to reduce outages in the systems that provide or support those services. Although we do not expect CDT to create measures for all state agencies, without developing measurable objectives in key areas, it is unable to effectively measure progress toward those goals or determine whether the State has met them.

CDT's previous strategic plan—in effect from 2017 through 2020—was slightly more detailed and included some objectives for achieving its broad goals. However, it also did not incorporate performance measures that CDT would use to evaluate progress. For instance, to achieve its broad goal of "create one digital government," CDT developed a priority to "accelerate the adoption of common technology platforms and shared services." However, the plan provided no indication of the specific actions that CDT or the State would take with respect to that priority or how CDT would determine success.

CDT asserted that it records its progress in implementing its strategic plan through the annual reports it publishes on its website, in which it provides highlights of statewide IT accomplishments and updates on performance metrics. However, the annual reports generally do not sufficiently indicate the extent to which a strategic goal was met or include measurements by which to interpret the metrics. For example, one of the statewide IT performance metrics CDT included in its 2021 annual report shows that the number of IT projects it approved increased from seven in 2020 to 11 in 2021. However, the annual report does not identify to which strategic goal this metric refers, nor does it provide context such as whether the 11 projects represent all or only some of the projects that the State was planning to undertake in 2021.

We found multiple examples of federal government agencies that followed the best practices that we have identified. For instance, the federal General Services Administration, whose mission includes delivering the best customer service and value in technology services to the federal government, has developed a strategic plan that identifies broad goals, measurable objectives, and performance indicators, as the text box shows.

Creating measurable objectives in one critical area would have been useful for tracking progress towards improvement. CDT has identified a need for qualified and experienced IT staff in state service, and it included a staffing-related goal in its current strategic plan. However, CDT did not identify in the plan any specific actions or initiatives to address this need. Further, it did not establish any metrics for measuring improvements in or worsening of the State's staffing situation. CDT's chief counsel indicated that the COVID-19 pandemic disrupted CDT's ability to develop metrics for its staffing-related goal. However, CDT's previous strategic plan, which it created before the COVID-19 pandemic, also included a staffing-related goal but similarly lacked measurable objectives for addressing this critical concern.

Example of Strategic Plan from the Federal General Services Administration

Strategic Goal 3 — Digital Government: A digital government that delivers for the public through trusted, accessible, and user-centered technologies.

Strategic Objective 3.2 — Lead government-wide adoption of shared technology solutions that improve digital governance, sharing, security, and interoperability.

Strategic Initiative 3.2.2 — Reduce public sector digital threats by expanding the Federal Risk and Authorization Management Program (FedRAMP).

Performance Goal 3.2.2 — Increase adoption of GSA-sponsored identity solutions.

Performance Indicator Definition:
(d) Number of Login.gov serviced applications:
This indicator measures the number of government services using Login.gov for identity verification.

Performance indicator 3.2.2 (d)

FISCAL YEAR	TARGET	RESULTS
2018	5	17
2019	34	46
2020	60	83
2021	100	199
2022	250	NA
2023	350	NA

Source: U.S. General Services Administration's 2023 Annual Performance Plan.

Although CDT hosts several IT leadership academies to develop public-sector IT professionals through in-person and virtual courses in IT leadership and project management, these efforts do not appear to have sufficiently addressed the State's staffing need. Our survey of state agencies indicates that hiring and retaining qualified IT staff is the greatest challenge that they currently face. For example, one survey response indicated that market conditions make recruiting and retaining IT talent difficult and that finding state staff who have experience and skills in the latest technology is challenging. Another respondent explained that IT staff with decades of experience have either retired or sought other opportunities, leaving a significant knowledge gap that will take years to address and that increases the time required to complete work. Further, CDT's reports on the IT projects it oversees have cited challenges in filling vacancies for critical IT positions, which can contribute to project delays.

In fact, some of CDT's own offices face significant vacancies. Specifically, according to data from CDT's human resources branch, as of August 1, 2022, CDT had a 14 percent vacancy rate overall with 153 vacancies among its roughly 1,000 positions.[4] However, CDT's Office of Digital Services (formerly Office of Enterprise Technology), the office within CDT that is responsible for developing innovative technology solutions had a 29 percent vacancy rate (23 vacant positions) while CDT's Office of Statewide Project Delivery, the office responsible for IT project planning and oversight had a 19 percent vacancy rate (19 vacant positions). CDT developed a plan in 2018 that included several initiatives to develop its own workforce for the subsequent three years, such as recruitment through social media channels and professional development through its leadership academies. However, the plan was in effect only through 2021. According to CDT's chief of human resources, CDT expects to release a new plan in 2023. Updating its workforce development plan will be important given that CDT estimated in 2018 that 45 percent of its workforce was either at retirement age or within five years of the average retirement age.

Examples of Survey Responses

"Some [CDT] directors had a better strategic vision than others but the department always appears to either lack the authority or willingness to use their authority, to achieve the strategic goals and objectives."

"Leadership and direction is only effective if it is actionable, rather than theoretical. Concepts are documented in a strategic plan but there is limited real communication or direction provided to departments in what the expected outcomes are."

"They provide a SIGNIFICANT amount of oversight in terms of compliance and rules, but they rarely provide strategic leadership in terms of guidance on emerging technologies."

Source: Survey responses.

The challenges with strategic planning practices we describe above align with a problem we identified nearly 10 years ago. In a September 2013 audit report, we found that CDT's strategic plan did not include sufficiently measurable goals or describe the specific tasks necessary to achieve its goals and objectives.[5] Our review during this audit demonstrates this weakness in CDT's planning remains.

Some survey respondents expressed concerns about CDT's strategic planning efforts, as the text box shows. These examples highlight the need for CDT to provide strong statewide strategic leadership that aligns with best practices to fulfill its mission.

[4] These data are from a point in time and do not align with the authorized position numbers in Figure 3 from fiscal year 2022–23.

[5] *High Risk: The California State Auditor's Updated Assessment of High-Risk Issues the State and Select State Agencies Face*, Report 2013-601, September 2013.

CDT Has Yet to Identify High-Risk, Critical IT Systems in Need of Modernization

CDT has also not properly addressed strategic management of at-risk IT systems. Effective September 2021, state law requires CDT to identify, assess, and prioritize high-risk, critical IT systems across state government for modernization, stabilization, or remediation. We include CDT's definitions of these terms in the text box. A critical IT system is typically one that is essential to the continuing operation of the agency that uses it. A high-risk IT system is generally one that faces the potential for an unplanned, negative business outcome involving the failure or misuse of IT, which can include outages, security breaches, or complete failure. An example that highlights the significant consequences of system disruptions and failures was reported in 2016, when the DMV experienced a system outage that affected 122 of its 188 offices. The outage—reportedly the result of a hard drive failure that overwhelmed DMV's network—left some offices unable to provide certain services for about two weeks, which affected its ability to process driver's licenses and vehicle registration transactions.

CDT's Definitions of Key Terms Related to the September 2021 Changes to Law

Modernization: Actions an organization takes to move away from an outdated and/or unsupported technology or process in order to adopt, adapt, or upgrade its technology to current industry best practices and/or standards to allow stable, scalable, and resilient support of the business needs.

Stabilization: Actions an organization takes to sustain and/or improve the reliability and availability of its current technology to efficiently support its current business needs.

Remediation: The act of correcting an error; mitigating a threat, vulnerability, or identified gap; responding to unexpected events; or preventing negative outcomes after an assessment of technology and/or the business process.

Source: CDT's documentation.

When we questioned CDT about its efforts to implement the new requirements, we found that it had not documented an overall plan or approach for how it would meet all of its statutory responsibilities. CDT has not developed a complete list of high-risk, critical IT systems and assessed them for modernization, stabilization, or remediation. Instead, it has taken a limited approach to identifying high-risk IT systems by focusing mainly on the stabilization aspect of the law. According to CDT's deputy director of critical services (critical services deputy), its initial approach was to ask agencies quarterly to nominate IT systems for stabilization. It then validated through an intake questionnaire whether the systems the agencies had identified were suitable for, and would receive value from, a stabilization assessment.

Once CDT has identified a high-risk system, its stabilization assessment process involves conducting interviews with key staff to learn about the system, gathering and analyzing system data, and drafting a report with results and recommendations. CDT asserted that it also addresses the remediation aspect of the law through its stabilization service. Specifically, after it has completed a stabilization assessment, it coordinates with the agency to develop a remediation roadmap to implement the recommendations in its report. As of January 2023, CDT had assessed a total of nine IT systems for stabilization, as Table 1 shows, and was in the process of remediating them, which it believes may take up to a year. CDT officials indicated they expect to complete the stabilization assessment cycle for all identified mission critical systems in four years. We were unable to assess the reasonableness of this estimate because they did not provide details about how many total systems require stabilization or how many CDT expects to complete each year. Thus, many of these systems may be at risk of failure and service disruption for several years.

Table 1
IT Systems and Their Respective State Agencies That Have Undergone CDT's Stabilization Assessment

	IT SYSTEM ASSESSED FOR STABILIZATION	STATE AGENCY
1	Electronic Adjudication Management System	Industrial Relations, Department of
2	Yountville Rector Reservoir System	Veterans Affairs, California Department of
3	Lotus Notes	Governor's Office of Emergency Services
4	Pest Damage Record	Food and Agriculture, California Department of
5	Lane Closure System	Transportation, California Department of
6	Examination and Certification Online System and CalCareers	Human Resources, California Department of
7	Oil Spill Prevention Database	State Lands Commission, California
8	Compensation and Restitution System	Victim Compensation Board, California
9	Environmental Complaint System	Environmental Protection Agency, California

Source: CDT documentation.

However, CDT plans to transition to a new approach in 2023. Specifically, the critical services deputy asserted that CDT plans to begin using information from the California Compliance and Security Incident Reporting System (Incident Reporting System) to identify critical systems that are at high risk and therefore require stabilization. The Incident Reporting System is managed by CDT's Information Security Office and is the State's single-source application for reporting, tracking, analyzing, and resolving information security incidents. Agencies record information about their mission critical systems in the Incident Reporting System, and data as of October 2022 identified 294 systems belonging to 60 different agencies. Data that CDT provided from the Incident Reporting System include preliminary National Institute of Standards and Technology (NIST) risk scores on state agencies' critical systems. CDT believes that using the NIST scores and other information it collects on system risks will enable it to more comprehensively and objectively identify risk than using a subjective nomination process. However, with data from only 60 agencies, the list is not complete given that there are 107 reporting entities. Further, CDT still must assess the systems to identify those that need to be stabilized or modernized.

Moving beyond stabilization, CDT has yet to establish and document a process to identify and assess IT systems that are outdated or difficult to support and require modernization, nor has it developed a timeline for doing so. Modernization is often a more significant process than stabilization. Although stabilization can sometimes involve a short-term fix, modernization of systems is often performed through an IT project that may take years and millions of dollars to complete. Although it is beginning the process, CDT has yet to develop or document a plan for creating an inventory of the State's high-risk, critical systems that may need to undergo modernization.

The September 2021 state law does not include a deadline for CDT's implementation of the new requirements. However, it does require CDT to submit an annual report to the Legislature of its progress, and that report is to include an explanation of how it is prioritizing its efforts. In January 2023, CDT published its annual report that highlights its progress in assessing the nine IT systems in need of stabilization. However, the annual report does not include a plan or any details of how CDT will identify, assess, and prioritize critical, high-risk IT systems for modernization. As noted in Figure A3 in our Appendix A, 53 agencies reported having at least one important system needing modernization, and 34 of these 53 reported at least having a second system with similar needs.

Although CDT acknowledged in its latest strategic plan that modernizing the State's legacy infrastructure is necessary, that plan does not provide any indication of how it will address such a challenge. Nonetheless, 53 of the 103 state agencies who responded to our survey indicated that they have IT systems—totaling more than 100 of varying size, complexity, and function—that they believe need to be modernized. One agency stated that many of its systems are at least 15 to 20 years old, use unsupported technology, and pose significant security risks. Another agency noted that its primary safety alarm system, which provides alerts about medical emergencies, is becoming obsolete: the equipment is aging and automating updates is difficult. These examples underscore the importance of CDT's identification and assessment of IT systems that require modernization. However, CDT has not yet met its statutory requirements to identify, assess, and prioritize high-risk systems to ensure that they are stable and up to date to meet the State's needs.

CDT Has Not Taken Adequate Steps to Minimize the Risk of Redundant Systems

As the text box shows, many agencies use systems that likely have similar functionality. However, CDT has not strategically managed these systems to ensure the efficient use of IT and to avoid potential duplication. State law directs CDT to minimize overlap, redundancy, and cost in state IT operations by promoting the efficient and effective use of IT. Additionally, one of CDT's strategic goals is to "make common technology easy to access, use, and reuse across government." Nonetheless, CDT acknowledged in its strategic plan that the State makes it easy for agencies to pursue individual projects instead of taking a collective approach to reusing technology. While these systems may serve unique purposes, there may be opportunities for sharing common functionality.

Examples of Possible Duplication of IT Systems

In its strategic plan, CDT reported that the State had the following systems:

- 79 case management systems across 22 agencies
- 45 reporting systems across 15 agencies
- 27 licensing systems across 23 agencies

In addition to these systems, common infrastructure needs range from document management and electronic signatures to identity authentication, verification, and validation.

Source: CDT's strategic plan *Vision 2023*.

Although CDT is responsible for approving the procurement of large IT systems, it has not established a catalog or process to enable agencies to take advantage of systems the State has already built or currently owns. Because CDT is responsible for approval decisions on large IT projects in the State, agencies submit information about those

projects to CDT. In fact, as of November 2022, CDT was in the process of reviewing 86 IT projects. CDT could use the information it receives about these projects to identify requests that involve potentially redundant or duplicative IT systems. However, CDT does not track and publish complete information that would enable reusability and minimize redundancy across IT proposals and projects, and it does not work with agencies to identify and pursue opportunities for sharing technology. CDT asserted that it is open to considering options for gathering this type of information in collaboration with other state agencies.

To its credit, CDT is collaborating with the State's Office of Data and Innovation to implement some aspects of reusability for IT. For instance, one of the Office of Data and Innovation's objectives is to leverage research, analytics, and insights to design reusable or scalable human-centered solutions for service improvements. In line with this objective, CDT and the Office of Data and Innovation have contributed to the creation of the California Design System (Design System), which is a combined effort with the Governor's Office and the California Government Operations Agency. The stated purpose of the Design System is to help digital teams solve common problems by pulling together reusable components and patterns as well as best practices. To this end, the Design System is aimed at developing reusable digital services for the State and is intended to obtain reusable components, patterns, and best practices for state agencies to develop user-friendly websites through its ongoing open-source project—an initiative to make digital information and services easier to use. For example, components of the Design System were reportedly used to create the website broadbandforall.cdt.ca.gov, a state initiative for improving broadband access to Californians. Although this reusability effort is generally limited to digital services such as websites, CDT could employ a similar approach for other IT projects it approves, such as licensing systems.

CDT Has Not Taken Critical Steps to Assess Whether Reporting Entities Have Implemented Appropriate Safeguards to Protect Their IT Systems

CDT has yet to determine the effectiveness of the cybersecurity programs that each of the State's 107 reporting entities have implemented. In the absence of comprehensive information, CDT does not have a clear picture of whether the State's IT systems as a whole are adequately protected (information security status). Further, most of the reporting entities CDT has reviewed are performing poorly, leaving state IT systems vulnerable to cyberattacks and other disruptions. Moreover, CDT has not done enough to promote its no-cost threat monitoring service, which hinders its goal of achieving better visibility of the State's threat monitoring efforts.

CDT Has Not Determined the Statewide Information Security Status

One of CDT's responsibilities is to oversee information security development for the State's 107 reporting entities. CDT has asserted that, for these information security programs to improve, it must be able to effectively measure the information security status both across the State and within each reporting entity individually.

Nonetheless, CDT has yet to fully assess the overall status of the State's information security. Further, information CDT has obtained indicates that most reporting entities are not making significant progress toward improving their information security. In the absence of such progress, cybersecurity threats, such as phishing and ransomware, can lead to costly disruptions in state services and the exposure of sensitive information. For example, in June 2022, a cyberattack shut down online access to CalJOBS, the Employment Development Department's (EDD) online job search center that claimants generally must use to receive unemployment benefits. In an even more recent example, the Department of Finance was the subject of a cyberattack in December 2022 in which data that may include social security numbers, bank account information, and user passwords were unlawfully obtained from its servers. Finally, from a global perspective, IBM Security reported the average total cost of a data breach in 2022 ranged from $2.1 million for the public sector up to $10.1 million for the health care industry.

As the text box shows, CDT relies upon a four-year oversight lifecycle consisting of technical assessments and compliance audits to objectively summarize each reporting entity's information security status into a single score, called a *maturity metric*.[6] However, because CDT has the capacity to complete only 13 compliance audits each year, which equates to 52 audits across the entire four-year lifecycle, it is not able to review all 107 reporting entities during a single oversight lifecycle. Consequently, CDT uses a risk-based methodology that considers various factors to prioritize the 52 highest-risk entities for review, such as the type of data that entities store, the nature of their business, the maturity of their overall information security programs, and their likelihood of facing threats that necessitate a high level of attention and monitoring.

CDT is currently scheduled to audit 52 entities through the new four-year cycle that began in July 2022 and that will end in June 2026. However, this total includes 35 entities from the prior lifecycle—which covered the period from July 2018 through June 2022—that CDT plans to continue monitoring. According to CDT's information security audit and assessment manager (audit manager), some of those 35 entities continue to be high risk because they have not shown enough improvement in their information security and others have missions that are so critical to the

The Components of CDT's Four-Year IT Security Oversight Lifecycle

One compliance audit: An information security audit that evaluates a reporting entity's compliance with state security and privacy policies by validating that its security systems, procedures, and practices are in place and working as intended. CDT stated that it has the capacity to perform 13 compliance audits each year.

One follow-up review: A post-audit follow-up to determine how much progress a reporting entity has made toward remediating the findings that CDT previously identified. CDT stated that it has the capacity to perform 13 follow-up reviews each year. CDT generally schedules its compliance audits and follow-up reviews in nonconsecutive years to provide reporting entities with time to obtain additional resources and to implement corrective actions to address audit findings.

Two independent security assessments: A technical assessment of a reporting entity's network and selected web applications to identify security vulnerabilities and provide implementable actions to reduce the possibility of security breaches. Reporting entities typically receive an independent security assessment every other year during the lifecycle. CDT currently contracts with the California Military Department to perform these assessments, although reporting entities may request permission from CDT to use a third-party vendor.

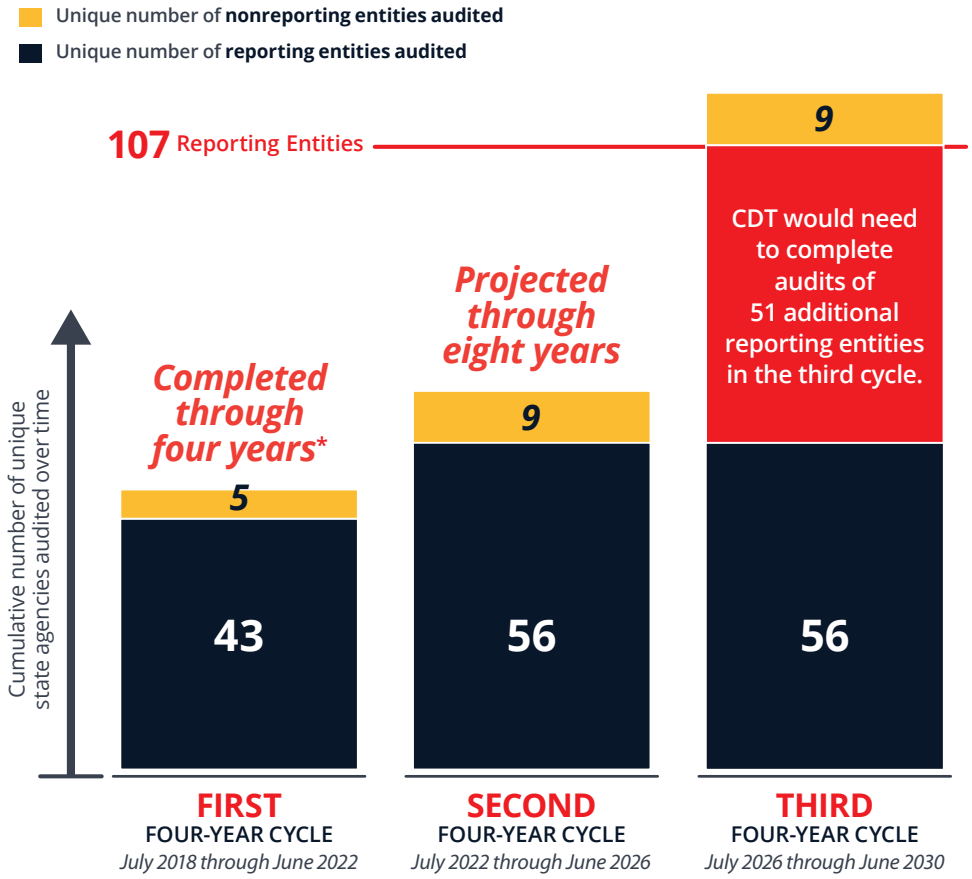
Source: Interviews with CDT staff and review of CDT's documents.

Note: Reporting entities do not receive an audit or follow-up review during the same year that they receive an independent security assessment.

[6] CDT invited some agencies that fall outside of its purview for information security oversight (nonreporting entities) to participate in its oversight lifecycle due to the interdependencies and data exchanges that exist between reporting and nonreporting entities.

State's business that major disruptions in their operations would be devastating. Nonetheless, by dedicating 35 of the 52 available audits during the current lifecycle to entities it has already reviewed, CDT is thus limiting itself to auditing only 17 additional entities over the next four years that it has not previously reviewed. Consequently, even though CDT had the capacity to conduct 104 audits during the first two lifecycles, Figure 5 shows that in the first four-year lifecycle CDT completed audits of 48 total agencies and in the second four-year lifecycle it is projected to increase that number by only 17 for a total of 65 agencies, of which 56 are reporting entities.

Figure 5
If It Continues to Follow Its Current Process, CDT Is Unlikely to Complete Audits of All Reporting Entities Until at Least 2030



Source: CDT's compliance audits.

* CDT completed only 48 of its 52 planned audits, and it did not complete all of these audits within the original four-year cycle. Specifically, CDT finalized five of these audits from July 2022 through September 2022.

As Figure 5 also shows, in the absence of any changes to its current process, CDT will not be able to complete audits for all reporting entities until June 2030. However, completing all 107 audits by June 2030 would require CDT not only to prioritize the remaining 51 reporting entities for its next oversight lifecycle but also to successfully

complete all those reviews in a timely manner. According to the state chief information security officer (state chief), CDT does not plan to audit all 107 reporting entities because it is not cost-efficient to look at smaller-scale entities that are typically less critical to the State or that have less complex information systems. However, when we followed up with CDT about which of the remaining 51 reporting entities it had identified as not warranting an audit, it was unable to provide us a listing of these reporting entities or a timeline for when it plans to complete audits for the reporting entities that do warrant audits. Although we confirmed that many of the 51 entities are small with respect to their number of employees, we noted that some of these entities have large budgets and some have access to sensitive information. Further, as the state chief pointed out, because of the interdependencies and data exchanges that exist between state agencies, the State's information security is only as strong as the weakest link. Consequently, even a small reporting entity may pose a risk to the State, which is why it is imperative that CDT determine which specific reporting entities warrant an audit and prioritize them for review.

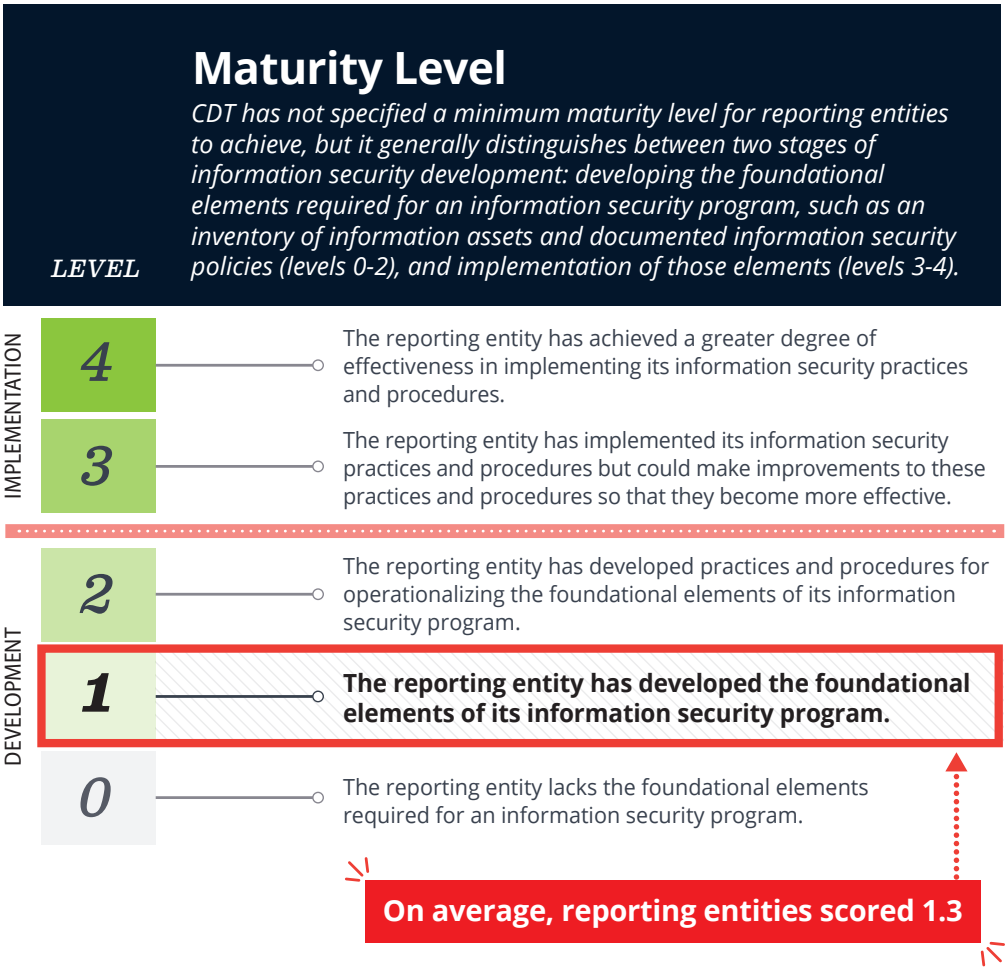
Regardless of whether it decides to audit all 107 reporting entities, CDT will still need at least the third lifecycle ending in June 2030 to review all the remaining reporting entities that warrant an audit. We find the lengthiness of this process concerning, particularly given how rapidly cybersecurity threats evolve. In fact, the manager of CDT's security risk governance unit (security risk manager) acknowledged that because risk is not static, a continuous monitoring approach is necessary to identify new high-risk findings that reporting entities need to address. Nonetheless, as we discuss later, we previously communicated our concerns to CDT about how long it is taking to develop an understanding of the State's information security status, and although CDT is exploring ways to speed up the process for establishing a statewide security status, it is still in the preliminary stages of these efforts.

Not only does CDT lack a comprehensive understanding of the State's information security status, but the information it has collected thus far shows that most reporting entities are at an early stage of their information security development. CDT had calculated maturity metrics for 43 of the 107 reporting entities as of December 2022. As Figure 6 shows, CDT found that on average, these reporting entities have achieved a maturity metric score of 1.3 out of 4, which means they have developed the foundational elements of their information security program, such as an inventory of their information assets and information security policies. However, they are still in the process of developing practices and procedures to implement their information security policies.

The purpose of CDT's compliance audits is to identify potential cybersecurity gaps and provide guidance to reporting entities on how to implement the State's information security and privacy policies. However, some reporting entities actually performed worse on reviews following their initial compliance audits, despite the increased oversight of their information security programs. Specifically, 28 of the 43 reporting entities for which CDT calculated maturity metrics received either a follow-up audit or another technical assessment, allowing CDT to update their initial maturity metrics to measure their progress. Only 12 of the 28 entities showed any improvement, and that improvement was minimal. Another 14 entities' scores declined, while the remaining two entities earned an exact repeat of their initial scores.

According to the security risk manager, a lack of resources—such as funding and skilled information security staff—is preventing many reporting entities from improving their information security. She explained that CDT has undertaken several initiatives to help reporting entities improve, such as implementing a cybersecurity boot camp and information security leadership academy programs to help participants develop and enhance their security and leadership skills. However, citing several published reports related to the information security job market, she explained that the challenge of recruiting skilled information security professionals will likely continue for another year or two.

Figure 6
Higher Maturity Metric Scores Reflect Higher Information Security Maturity Levels



Source: Interviews with CDT staff and review of CDT's maturity metrics.

Although CDT recognizes that some reporting entities have resource constraints that make it challenging to implement timely corrective actions, the deputy state chief information security officer (deputy chief) stated that these excuses can no longer get in the way of shoring up known deficiencies. Therefore, he explained that

CDT wants to come up with a mechanism for holding reporting entities accountable for addressing known shortcomings in their information security programs. For instance, CDT could require entities that fail to meet minimum security maturity levels to use CDT's services, such as its no-cost threat monitoring service that we discuss in the next section or its advisory service whereby CDT's information security advisors work with a reporting entity short-term to address predictable weaknesses with their information security. Similarly, when appropriate, CDT could require reporting entities to address outstanding information security deficiencies before implementing new IT initiatives.

In our January 2022 report, we concluded that CDT's progress toward determining the State's information security status has been hampered by its delays in completing its compliance audits.[7] To ensure that it is able to determine this status, we recommended that by June 2022, CDT increase its capacity to perform compliance audits of high-risk reporting entities. We noted that this change could entail CDT hiring more staff or securing additional contracted audit support. However, according to CDT's audit manager, it continues to maintain the same capacity of reviewing 52 entities during its current four-year oversight lifecycle using its existing team of six auditors and five research specialists.

Consistent with its response to our January 2022 report, the deputy chief explained that CDT does not have any immediate plans to hire more audit staff to increase its capacity for performing timely compliance audits; instead, it hopes to implement a new IT system and become more efficient at conducting audits so that it will be able to conduct audits of all entities more frequently. Specifically, the audit manager explained that by regularly requiring reporting entities to upload documentation into the new system showing evidence of their information security controls and keeping everything up to date, CDT staff will no longer have to coordinate with the reporting entities to obtain those documents at scheduled intervals. Further, she stated that CDT will be able to use artificial intelligence capabilities within the system to automate its review of content in the documents, which will reduce the amount of human validation required to ensure that reporting entities are compliant with various information security requirements. However, the deputy chief stated that CDT still has not secured the necessary funding for a new IT system, and as we noted in our previous report, a new system's implementation can take several years.

In the meantime, CDT has identified certain steps it may take. Specifically, in response to our current audit, CDT is considering hiring a contractor to determine whether it can increase the efficiency of its existing process. Further, the security risk manager explained that CDT is currently developing a new priority risk ranking process that will allow it to quickly develop a baseline information security score for all reporting entities without having to complete compliance audits for each. This score will summarize readily available information, including the results of the reporting entities' independent security assessments as well as information that the reporting entities self-report annually to the federal government. We previously

[7] *State High-Risk Update—Information Security: The California Department of Technology's Inadequate Oversight Limits the State's Ability to Ensure Information Security,* Report 2021-602, January 2022.

recommended that CDT use this self-reported information to help develop its understanding of the statewide information security status. Although this score will provide useful information on reporting entities that CDT has yet to audit, it does not replace the need to establish maturity metrics, which are fully based on independently validated information, including compliance audits. CDT intends to use its priority risk ranking process to augment its maturity metrics scoring process. Finally, the state chief explained that developing a baseline information security score will allow CDT to identify common gaps that exist in the State's information security and can inform the areas where CDT offers additional guidance and support.

Although the security risk manager stated that CDT intends to start establishing the priority risk ranking process scores as early as the first quarter of 2023, she noted that it has yet to finalize its preliminary work products. Consequently, we do not have assurance that CDT will meet its timeline. If, as CDT asserts, understanding the State's current information security status is required to implement effective improvements, then it will be taking a great risk if it maintains the status quo and prolongs its efforts to determine the types of information security deficiencies that exist across the State.

CDT Could Do More to Promote Its No-Cost Threat Monitoring Service

As prescribed by CDT's information security requirements in the *State Administrative Manual* and the *Statewide Information Management Manual*, state agencies are ultimately responsible for conducting their own monitoring for cybersecurity threats; however, CDT provides support to assist in those efforts. For example, in accordance with industry best practices, CDT partners with multiple federal, state, local, and private entities to share threat intelligence and manage cybersecurity threats and incidents. Further, CDT offers a cybersecurity threat-monitoring service at no cost to state agencies. The chief of CDT's security operations center (security operations chief) explained that having all state agencies participate in the threat monitoring service would give CDT better visibility into the State's threat monitoring efforts.

Beginning in July 2021, CDT started offering its threat monitoring service at no cost to all state agencies. Agencies using the service work with CDT to implement continuous streaming of their security-related logs to CDT for it to perform around-the-clock monitoring to detect cybersecurity threats. These logs provide a record of the events occurring within the agency's information systems and networks. CDT compares the activity in the logs to known tactics and techniques used in cyberattacks. When CDT identifies indications of a possible cyberattack, an analyst reviews the information, and when a cyberattack cannot be ruled out, it notifies the affected agency of the potential threat. According to the security operations chief, CDT's threat monitoring service helped identify 36 confirmed incidents during a recent 10-month period.

The deputy chief explained that CDT's threat monitoring service could benefit individual agencies as well as the State as a whole. For example, he stated that one objective of the service is to mitigate threats for those agencies that cannot

adequately conduct their own monitoring because of internal constraints, such as a lack of personnel or technological resources. Further, he noted that distributing the State's available funding for threat detection across all state agencies is inefficient. Rather, having CDT provide centralized threat monitoring services for more state agencies would require fewer resources overall and improve the State's ability to monitor threats and alert agencies statewide as necessary.

Despite the potential benefits of its service, CDT has not done enough to inform state agencies of this resource. In fact, as of January 2023, the security operations chief confirmed that only 23 of the 107 reporting entities were using the service. Our survey found that some state agencies have opted not to use CDT's service because they are currently under contract with a vendor that provides threat monitoring services or because they have already established their own internal process. Some agencies stated that CDT's service was unable to meet their specific needs, while only 28 percent of surveyed agencies reported using CDT's monitoring service.

Although CDT has made efforts to inform agencies about its threat monitoring service, many agencies have not signed up. The deputy chief explained that, in addition to describing the service on its website, CDT relies upon presentations, trainings, and meetings with agencies' information security personnel to educate them about its monitoring service. However, CDT could perform more outreach to increase awareness. In fact, the deputy chief stated that CDT is considering scheduling individual meetings with agencies to inquire about their current approaches to monitoring cybersecurity threats. In addition, the security operations chief stated that CDT is considering issuing a policy to formally recommend that agencies use its threat monitoring service but that the policy would not mandate the service's use because some larger agencies have been effectively performing their own internal threat monitoring for a long time. However, CDT has not formally started developing such a policy.

CDT announced in October 2021 that to increase the State's ability to detect, protect against, and respond to cybersecurity threats, it will require reporting entities that are already conducting their own threat monitoring to work with CDT to develop the most effective ways to exchange threat information with CDT by the end of 2023. The deputy chief stated that CDT will encourage all other state agencies to use its threat monitoring service. Regardless, until CDT can consistently obtain threat monitoring data statewide, it will continue to lack comprehensive knowledge about the types of threats that exist across the State's information systems. This knowledge gap may weaken CDT's ability to plan and prioritize the State's response to significant information security threats.

CDT's Approval and Oversight Processes Do Not Adequately Mitigate Risks for Complex IT Projects

CDT designed its project approval lifecycle (PAL) process and independent project oversight (project oversight) to mitigate the significant consequences of failed IT projects. Nonetheless, the PAL process misses important opportunities to identify and address potential risks during project planning. Further, when providing project oversight, CDT has not adequately intervened when ongoing risks have begun to negatively affect

projects. Consequently, many complex projects that have gone through CDT's PAL process and project oversight have experienced schedule delays, cost overruns, issues with system functionality, and significant differences between expectations and project outcomes that CDT might have identified and resolved sooner. These outcomes call into question the effectiveness of CDT's approval and oversight efforts.

CDT's PAL Process Is Not Achieving Its Intended Purposes

State law makes CDT responsible for approving IT projects. As we explain in the Introduction, CDT has generally delegated to state agencies the authority to approve their own IT projects under a dollar threshold that CDT establishes based on its assessment of the agency's project management and project performance (delegated IT projects). In contrast, agencies must obtain CDT approval for IT projects over their threshold or for any project of more than $5 million (nondelegated IT projects). To ensure that all nondelegated IT projects include a strong business case, clear business objectives, accurate costs, and realistic schedules, CDT approves them through the PAL process. The PAL process has four stages, as the text box shows. A nondelegated IT project can begin execution only after CDT has approved all of the four stages. As of November 2022, CDT's website listed 86 proposed projects in one of the four stages of the PAL process. CDT's annual reports indicate that it has approved 51 projects using the PAL process since 2016.

The Four Stages of PAL

Stage 1—Business Analysis: Communicates the business investment justification by describing factors including statutes or legislation, program background and context, business problems or opportunities, and strategic business alignment.

Stage 2—Alternatives Analysis: Evaluates multiple alternative solutions and determines which solution will yield the highest probability of success.

Stage 3—Solution Development: Acquires a solution that best meets business objectives and yields the highest probability of success.

Stage 4—Project Readiness: Evaluates and reconfirms that the business objectives will be achieved, ensures that the solution selected continues to yield the highest probability of success, and baselines the project's time frames, projected schedule, and costs.

Source: *State Information Management Manual.*

According to CDT, the PAL process entails its staff working closely with state agencies to assist them in completing required materials for project approval and to ensure that project proposals are well thought out and clearly indicate program benefits. CDT intends for the PAL process to achieve several purposes, including the following:

- Better business outcomes for the State through successful IT projects.
- More successful projects and fewer revisions to project plans.
- The introduction of scalability to the project approval process based on business and/or technical complexity.

CDT fully implemented the PAL process in 2016 to replace its previous approval process—the Feasibility Study Report process—after several IT projects that were approved through that process experienced problems that led to significant cost increases and schedule delays. One example was the State Controller's Office's 21st Century Project, MyCalPays. The State Controller's Office ultimately terminated the contract of the vendor implementing that system after the State had spent more than $200 million over nearly nine years.

We identified several concerns with the PAL process that call into question whether it is effectively achieving its intended purposes. First, CDT may be missing an opportunity to require agencies going through the PAL process to consider modern system development approaches in order to reduce project size, which, in turn, could reduce financial risk, procurement time, and implementation time. Modern approaches to IT projects, such as agile or modular approaches, take a smaller and more incremental path than the traditional waterfall approach in which an agency deploys an IT system all at once at the end of the project. However, not only does the PAL process not require agencies to determine whether an agile or modular approach would be optimal, but some agencies indicated through our survey that PAL lacks the flexibility to accommodate these approaches. Our IT expert stated that the single most effective change to improve the odds of success is to decrease the size of the projects attempted, where feasible; the IT industry and the federal government have similarly concluded that smaller projects are less risky. In fact, Congress enacted a law in 2011 that states that executive agencies should use modular contracting for the acquisition of major IT systems to the maximum extent practicable, which divides what would be a large contract into several shorter-term, lower-cost contracts by separating entire IT systems into smaller modules. CDT believes that PAL has the flexibility to allow agencies to select an adaptive or agile development process. However, the current process does not explicitly require agencies to consider such approaches.

Another limitation is that the PAL process is not designed to ensure that IT projects align with statewide strategic goals. We expected that CDT would use the PAL process to ensure that proposed projects align with its strategic plan's stated goals. However, Stage 1 of PAL requires an agency to describe how the proposed project will help achieve only the agency's strategic business plans, rather than statewide IT strategic goals. Further, for many large agencies, CDT delegates approval of Stage 1 to the agency's information officer, forgoing the opportunity early in the process to verify that the proposed project aligns with statewide strategic goals.

Not adequately ensuring that projects align with the statewide IT strategy may have contributed to the need for EDD to restart its Benefits Systems Modernization project (EDD's modernization project) using a different approach. EDD's modernization project is a critical and large integration of EDD's unemployment and disability insurance benefit systems. During the COVID-19 pandemic, the Governor directed a strike team of experts with experience in solving complex service delivery, operations, and technology problems to review EDD's struggles to process unemployment insurance claims in a timely manner and to reduce its backlog. The strike team reviewed EDD's modernization project, which was in the final stage of PAL at that point. It recommended that EDD restart the project using a more iterative modernization approach that prioritizes EDD's most critical needs—an approach that CDT could have encouraged during the early stages of the PAL. The strike team also recommended that the project focus on a customer-centered design, a state strategic priority that CDT should be considering during the PAL process.

Consequently, the project's original proposed start date of October 2020 has been delayed at least two years, further prolonging this key system modernization. In June 2021, CDT approved the project to reengage planning activities, and it is

currently in Stage 1 of the PAL process. The delay in the modernization of this key system may have a tangible impact on Californians who rely on EDD to promptly process their claims.

Another concern we identified with the PAL process is that it is time-consuming. CDT declared in its strategic plan for 2017 through 2020 that it would increase operational performance by accelerating the planning-to-execution cycle time for projects, which suggests it intended to shorten the length of time necessary for approval through PAL. However, in response to our survey, several agencies stated that the PAL process is too lengthy and delays the approval of projects. CDT has not developed formal policies for the expected length of review for each PAL stage. Although we acknowledge that projects differ in size and scope, completing all four stages of PAL for the three projects we reviewed that were approved through PAL took 11 months for one project and nearly four years for each of the other two projects. Timelines that stretch into multiple years can be costly to agencies and delay updates to critical systems.

Our review of four procurements, which CDT evaluated in Stage 3 of PAL, found that CDT followed key provisions of the law and policies in managing them but that its process took a significant amount of time. CDT conducts and oversees statewide IT procurements related to IT projects, including ensuring compliance with laws and policy, performing negotiations of contracts, and communicating with vendors. The procuring state agency must participate in all steps, including developing the statement of work that captures the contractual obligations between the State and the vendor. The procurements we reviewed adhered to key components of state law, including the issuance of requests for proposals, an allowable contract negotiation process, and payment withholding until final delivery or acceptance of the goods or services. CDT also documented that members of its evaluation team that selected the vendors for these projects had signed confidentiality and conflict-of-interest forms, as policy requires. However, CDT does not have documented expectations of the timeliness of its procurement reviews; instead, it indicated that procurement timelines are driven by the agency involved, not policy. The actual timelines for two of these procurements were quite lengthy—22 months and 30 months.

Underscoring our concerns, CDT has not, to date, measured the effectiveness of the PAL process. CDT stated that the success of the PAL planning process can be inferred based on information in its oversight reports and the special project reports that the agencies issue. However, we do not believe that such an approach, which lacks a documented analysis, is sufficient. A February 2017 report from the Legislative Analyst's Office recommended that CDT report at budget hearings on the quantitative and qualitative measures it planned to use to evaluate the effectiveness of PAL and the success of state IT projects. Similarly, in our state high-risk report from August 2021, we concluded that CDT had not demonstrated that PAL had been effective on highly critical and complex projects.[8] Nonetheless, as of November 2022, CDT continued to be unable to provide a documented approach to measuring the

[8] *The California State Auditor's Updated Assessment of Issues and Selected Agencies That Pose a High Risk to the State,* Report 2021-601, August 2021.

effectiveness of PAL. Because CDT requires nondelegated IT projects—often with costs in the multimillions of dollars—to complete the PAL process, the State needs to be certain that the process is effective.

CDT's Independent Project Oversight Continues to Be Ineffective at Addressing Risks on Complex Projects

Independent project oversight is essential to help ensure that IT projects comply with approved project plans and objectives, including cost, schedule, and scope. According to the *State Administrative Manual* and the *Statewide Information Management Manual*, CDT will perform project oversight on medium- and high-criticality IT projects for agencies and constitutional offices. As of November 2022, CDT was overseeing 29 IT projects for 20 different agencies, with an estimated total cost of $3.7 billion.

CDT has significant authority to intervene in IT projects to ensure that they comply with approved objectives. For instance, CDT has the authority to require agencies to perform the remedial measures listed in the text box. CDT also has the authority to suspend, terminate, or reinstate IT projects. Moreover, it can establish restrictions to mitigate nonperformance by agencies, such as requiring them to demonstrate successful correction of identified performance failures before it approves future projects.

Examples of Remedial Measures CDT May Require

To ensure that IT projects comply with objectives, CDT may require an agency to take one or more of the following actions:

- Conduct an independent assessment of project activities.
- Establish a remediation plan.
- Provide additional reports on the project.
- Seek CDT's approval before initiating actions in the approved project schedule.

Source: State law.

Despite its significant authority, CDT did not always adequately intervene in the projects we reviewed to ensure that the agencies resolved the problems that its project oversight identified. When we reviewed CDT's project oversight reports from the four IT projects described in Table 2, we found that CDT had identified that all four had ongoing risks and problems. Appendix B summarizes the contracts for these four projects and the associated amendments. Further, CDT reported that three had deficiencies that required immediate corrective action. We provide an example of the history of one such project in Figure 7. According to CDT, its general oversight approach is collaborative, iterative, and incremental. CDT stated that the objective of its oversight work is early engagement to help identify risks and issues, and to make recommendations to mitigate risks and resolve issues, thereby resulting in minor corrective actions that can reduce the occurrence of the highest CDT-directed corrective action plans or project suspension or termination. Although CDT identified significant problems in the IT projects we reviewed, it has not used its available authority to ensure the resolution of those problems. In fact, CDT could not provide evidence that it had used its suspension, reinstatement, or termination authority for any project since 2016. Table 2 also shows information about the cost, schedule, and status of the projects we reviewed.

Table 2
IT Projects We Reviewed Experienced Changes to Their Cost and Schedule

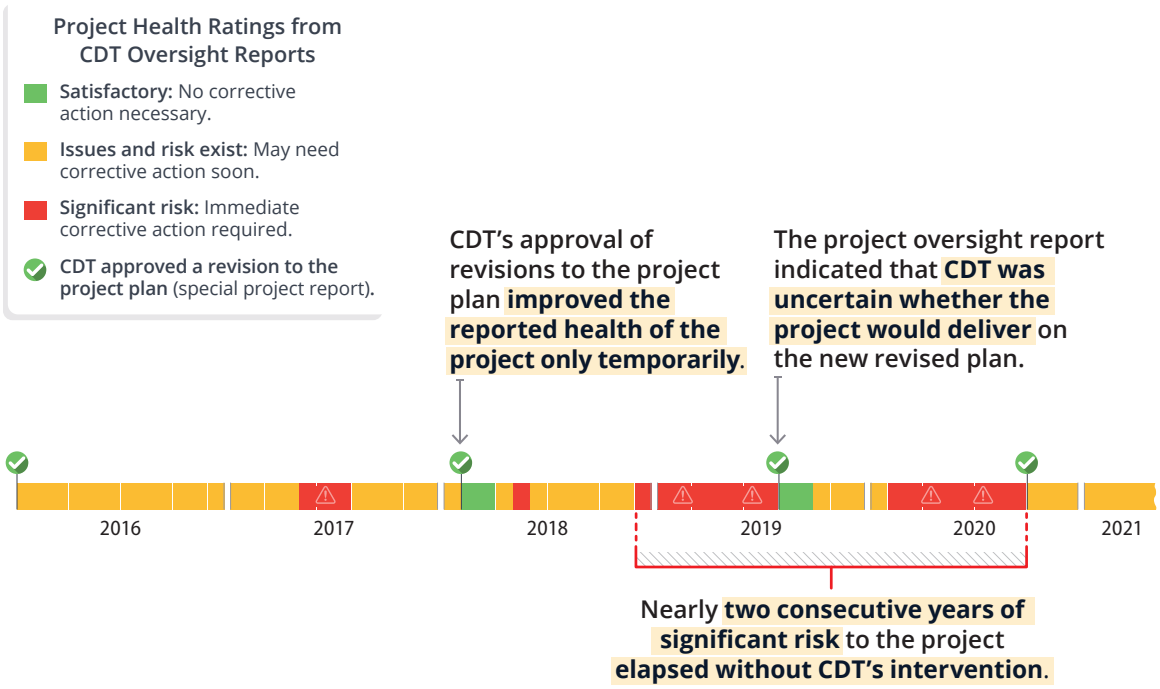
PROJECT	DEPARTMENT	DESCRIPTION	COST	SCHEDULE	STATUS
Child Welfare Services—California Automated Response and Engagement System (Child Welfare System)	California Department of Social Services	Aims to replace the existing legacy child welfare systems, including the case management system and licensing system, which entails streamlining workflows to alleviate obstacles that prevent child welfare workers from spending time with children and families.	Original estimate: $392.7 million Current estimate as of January 2023: $911 million	Project start: July 2013 Original estimated project end: September 2017 Current estimated project end: July 2025	As of January 2023, CDT had rated the overall project health as red, indicating that immediate actions are needed to address significant risks to project health.
Transportation Asset Management System	California Department of Transportation	Aims to develop a repository of information about California's transportation assets, such as pavement, bridges, and culverts on state highways, to better prioritize and facilitate repair work and new construction.	Original estimate: $28.3 million	Project start: December 2020 Original estimated project end: March 2024	Vendor contract terminated August 26, 2022 CDT reported that the project is seeking a new vendor.
Digital eXperience Platform	DMV	Aims to modernize legacy systems to transform and streamline DMV services delivery to Californians.	Original estimate: $414.7 million	Project start: September 2021 Original estimated project end: June 2026	As of November 2022, CDT rated the project's overall health as yellow, indicating that there may be a need for corrective action in the near future to address existing risks and issues. It noted that risks will continue to be high with the very tight schedule and zero contingency built in, increased scope, and continued high resource vacancy rate.
Financial Information System for California (FI$Cal)	Department of FISCal	Combines the State's accounting, budgeting, cash management, and procurement operations into a single financial management system.	Original estimate for statewide system in 2006: $1.3 billion* Cost estimate after implementation approach was updated in 2012: $616.8 million Actual total cost as of the end of June 2022: $960.2 million	Project start: December 2006 Original estimated project end: June 2015 Actual completion: July 2022†	State law determined FI$Cal's objectives to be complete as of July 1, 2022. The project has a reduced scope and state agencies struggle to use FI$Cal, which has contributed to delays in the State's financial reporting. Not all state agencies have transitioned to FI$Cal.

Source: Project documentation and CDT's project oversight reports.

* Although the project was initiated as the Budget Information System in 2005, the scope was transformed in 2006 to FI$Cal.

† Deemed "complete" through statutory action, AB 156 (Chapter 569, Statutes of 2022).

Figure 7
CDT Did Not Adequately Address Issues and Risks That It Identified for the FI$Cal Project



Source: *State Information Management Manual*, CDT's project oversight reports, and special project reports for the FI$Cal project.

Note: A new law, AB 156 (Chapter 569, Statutes of 2022), went into effect September 27, 2022, that deemed the FI$Cal project's objectives for certain reporting purposes to be complete as of July 1, 2022. Therefore, no further oversight reporting by CDT on system development, implementation, enhancement, maintenance and operations, security, or related workload is required for FI$Cal.

Moreover, CDT did not use its authority to require any of the agencies for these four projects to develop a corrective action plan to get their IT projects back on track, even when the projects exhibited conditions that should have necessitated corrective action. According to the *State Information Management Manual*, CDT may require a corrective action plan at any point in a project to alter the project's course or to change specific tasks that are not consistent with the most recently approved project plan. The manual also states that intervening early with minor and prompt corrections can be more effective than waiting until a project requires more significant corrective actions. However, CDT was unable to provide any examples of corrective action plans it required these agencies to provide. CDT asserted that it has worked with agencies as they have required corrective actions from their vendors, and some of its escalation of oversight is verbal and is not documented. Nevertheless, by not requiring agencies to prepare and provide a corrective action plan that shows how they addressed the concerns CDT identified, CDT is not holding them accountable.

Rather than using its authority to require a corrective action plan when problems arose for two of the four projects we reviewed, CDT relied on the agencies to produce special project reports. However, these reports did not address the underlying risks and issues facing the projects. CDT usually requires an agency to submit a special

project report whenever a project substantially deviates from the costs, benefits, or schedules documented in its most recent project approval document, as well as in other circumstances. The special project report process can redefine a project's cost, schedule, or scope. CDT describes this process as establishing a new baseline for measuring project progress and performance going forward.

Although this type of *rebaselining* can improve perceptions of project health in the short-term, the perceived improvement is likely to be short-lived if the agency has not resolved the root cause of the problem. Figure 7 shows the worsening of project health ratings following CDT's approval of FI$Cal's special project reports. Furthermore, after a rebaselining, CDT no longer measures or tracks the project against its original approved plan. Consequently, rebaselining can obscure significant changes to a project's initial schedule, cost, and scope, potentially misleading the public on the project's actual performance.

In eight reports over the past 10 years, we have documented CDT's history of not sufficiently intervening to resolve ongoing problems in IT projects. For example, we reported in 2015 that CDT's project oversight identified roughly 180 significant and persistent concerns over a nearly four-year period with the BreEZe IT project.[9] The Department of Consumer Affairs intended for this project to provide a system that supported regulatory agencies' applicant tracking, licensing, renewal, enforcement, monitoring, cashiering, and data management capabilities for professional and vocational occupations. Given the significance and number of concerns raised, CDT should have fully analyzed the costs and benefits of suspending or terminating the project versus proceeding. However, it did not take sufficient action to ensure that the agency appropriately addressed the concerns. Consequently, the estimated total costs of the project increased from $28 million in 2009 to $96 million in 2015, for implementation of a system that included only half of the regulatory entities originally planned.

Our other reports on CDT documented similar problems. For example, in 2017 we reported that its project oversight staff lacked clear guidance for when to escalate problems to its management.[10] In addition, we found that CDT lacked criteria for the conditions that would lead it to consider suspending or terminating projects.

Further, our numerous reports on FI$Cal have noted ongoing concerns with schedule, cost, and project functionality that were not adequately addressed. For example, we reported in August 2018 that in its oversight report CDT identified significant risks in the areas of time, resource, and risk management for FI$Cal, and it recommended in that report that FI$Cal's steering committee consider delaying the implementation of FI$Cal at 64 state agencies until these problems are resolved.[11] However, CDT did not share these concerns with the steering committee and did not publish its oversight report until one day after the project's steering committee

[9] *California Department of Consumer Affairs' BreEZe System: Inadequate Planning and Oversight Led to Implementation at Far Fewer Regulatory Entities at a Significantly Higher Cost,* Report 2014-116, February 2015.

[10] *High Risk: The California State Auditor's Updated Assessment of High-Risk Issues the State and Select State Agencies Face,* Report 2017-601, January 2018.

[11] *FI$Cal Status Letter*, Report 2017-039.1, August 2018.

had already decided to move forward with the implementation. In subsequent years, the project struggled to implement FI$Cal at various agencies, resulting in further revisions to the project schedule.

In addition to the weaknesses in its project oversight, CDT does not track and analyze lessons learned from completed or terminated IT projects. Agencies must prepare and submit to CDT a post-implementation evaluation report for completed IT projects to document lessons learned for use in future projects. However, state policy does not require such reports for projects that have not been implemented; therefore, a terminated project would not result in this report being produced, potentially depriving CDT of valuable information. The state chief project officer and deputy director of CDT's Office of Statewide Project Delivery indicated that CDT is currently working to capture lessons learned in a searchable statewide IT project knowledge database for CDT and agency use. However, although CDT asserts that it has considered lessons learned from past projects when revising its policies, it does not have a documented process or plan for analyzing the lessons learned from the agencies' post-implementation evaluation reports. Thus, it is less able to identify common challenges and revise or improve its IT project oversight policies or procedures. In essence, CDT is forgoing an opportunity to develop best practices for current and future projects that would likely improve those projects' chances of success.

CDT's Ability to Independently Oversee IT Projects Is Compromised

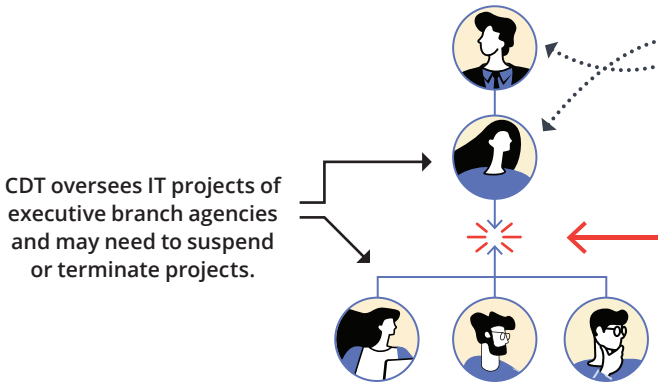
Under the State's current structure for IT project oversight, CDT's independence is compromised, limiting the effectiveness of its efforts. In terms of project oversight, independence is the freedom from conditions that threaten the ability of an oversight agency to carry out its responsibilities in an unbiased manner. Since 2009 we have raised concerns about CDT's ability to maintain its independence and the effectiveness of its IT project oversight, yet CDT continues to face these problems. As we previously describe, CDT was unable to demonstrate that it used its authority to require a project to provide a corrective action plan, and it has not suspended or terminated a project since 2016. Its pattern of not taking adequate action when projects are struggling illustrates our concerns about its ability to make difficult decisions that are in the State's best interests, such as by suspending or terminating high risk projects.

Best practices recognize two key types of independence: organizational independence and technical independence. As Figure 8 illustrates, CDT's independence is compromised in both of these areas. Organizational independence requires an agency that provides oversight to be departmentally and hierarchically separate from the agency managing the project. In other words, the oversight agency must be free from adverse pressures, direct or indirect, from the agency it is overseeing. CDT's organizational independence is impaired by the fact that although it is departmentally separate from the agencies it oversees, it is not hierarchically separate: it is an executive branch department that reports to the Governor and is overseeing IT projects of other executive branch entities.

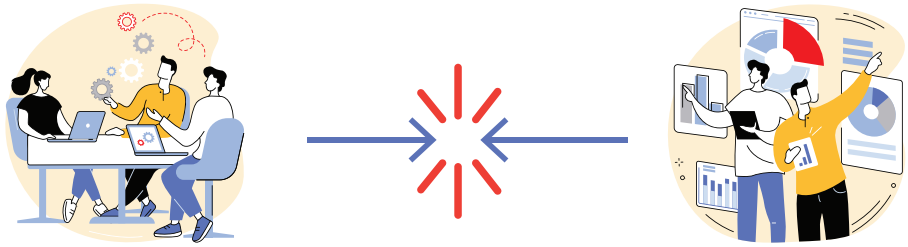
Figure 8
The State's Current IT Project Oversight Structure Compromises CDT's Independence

CDT's duty to consult with and assist state agencies conflicts with its duty to oversee IT projects.

Organizational Independence



Technical Independence



Source: State law, *State Administrative Manual*, *Statewide Information Management Manual*, U.S. Government Accountability Office *Government Auditing Standards*, The Institute of Internal Auditors best practices, Institute of Electrical and Electronics Engineers best practices, State Auditor past reports, and CDT documentation.

CDT believes it is insulated from threats to independence because of its organizational placement and reporting relationships. However, persistent project oversight issues are ultimately escalated to CDT's directorate—consisting of CDT's director and certain deputy directors—who decide whether to issue a corrective action plan to a project or to suspend or terminate it. The director also has the statutory responsibility to advise the Governor on the strategic management of the State's IT resources, which creates a potential conflict with CDT's ability to carry out its oversight activities in an independent manner.

Regarding technical independence, best practices recommend that oversight staff not participate in a project's initial planning. In 2014 we reported the possible conflict between CDT project oversight staff's responsibility to oversee IT projects and their responsibility to provide lessons learned and advice to the agencies that are completing the projects.[12] We continue to have these concerns because the same CDT oversight staff are responsible for project approvals and oversight. These staff work closely with an agency to complete the PAL process and then must provide project oversight that might require criticizing the planning that they participated in or even escalating issues that might lead to suspending or terminating the project. The problems that can arise from oversight situations of this nature are sometimes referred to as the "threat of self-review." In CDT's case, the blurring of the planning and oversight roles may create conflicts and compromise objectivity for CDT staff.

[12] *High Risk Update—California Department of Technology: Lack of Guidance, Potentially Conflicting Roles, and Staffing Issues Continue to Make Oversight of State Information Technology Projects High Risk,* Report 2014-602, March 2015.

Blank page inserted for reproduction purposes only.

Conclusions and Recommendations

As Figure 9 shows, CDT has not ensured its own or other state agencies' accountability in achieving the State's IT strategic goals. Further, CDT has not prioritized its critical responsibilities or acted with urgency in addressing pressing issues and risks. Finally, CDT's ability to provide effective IT project oversight is limited by impairments to its independence.

Figure 9
CDT Has Not Demonstrated Critical Leadership Qualities

Source: State and federal best practices.

We believe that prompt action is necessary to address these foundational and structural weaknesses. The measures we recommend on the following pages will clarify CDT's priorities and help it become more proactive in addressing the State's IT needs. Some of the recommended changes will affect CDT's staffing, which may require it to determine whether staff augmentations or reassignments are necessary to right-size its staffing resources and align them with its priorities.

CDT Must Better Ensure Accountability for Achieving the State's IT Strategic Goals

According to best practices, strong leadership requires accountability for measurable high-quality, timely, and cost-effective results. By not conducting performance monitoring or evaluations of its strategic goals, CDT has omitted accountability—a critical component—from its strategic planning process. This significant omission inhibits the State's ability to meet its goals for IT. CDT officials indicated that CDT does not directly manage departments, nor does it set IT prioritization at the department level. They further stated that CDT takes a leadership role and develops, communicates, and facilitates statewide IT strategic direction.

However, this position demonstrates that CDT fundamentally misunderstands its role in strategic planning. State law clearly directs CDT to take all appropriate and necessary steps to implement the State's strategic IT plan. As the statewide leader for IT, CDT is well positioned to implement accountability measures that track the State's progress. Specifically, CDT should ensure that its IT strategic plan aligns with best practices, includes measurable objectives related to its broad goals, and incorporates concrete performance measures.

CDT Must Prioritize Its Responsibilities

CDT should prioritize its responsibilities in addressing the critical IT issues affecting the State. Prioritization includes focusing efforts in key areas when goals or due dates are in conflict, as well as championing and providing adequate resources for change. Addressing the statewide IT staffing shortage should be one of CDT's top priorities. To mitigate this shortage, CDT should identify root causes in areas such as salaries or recruitment approaches, work with state agencies and industry stakeholders to propose solutions, and monitor the results of its and state agencies' staffing efforts.

CDT should also prioritize developing a plan to identify and assess IT systems that may require modernization. When we spoke to CDT, its officials did not have a clearly defined and documented strategy for addressing the statutory requirement regarding modernization, conveying instead that its approach was evolving. It asserted that state agencies can self-identify the need to modernize their systems and apply for funding through the Technology Modernization Fund, which agencies can use to fund a small project that can provide high-value services quickly or that can serve as a proof-of-concept to jumpstart large projects approved through PAL. However, the law is clear that CDT has the responsibility

to identify, assess, and prioritize high-risk, critical IT systems for modernization. Therefore, CDT should develop a detailed plan by July 1, 2023, of how it will satisfy its statutory requirements.

Finally, to avoid costly duplication of efforts related to IT projects and systems, CDT should prioritize creating a catalog of reusable systems and components of systems statewide. Maintaining such a catalog could help CDT determine when requests for IT projects duplicate already existing IT systems or their components. This information would contribute to the efficiency of IT statewide and would likely reduce the costs associated with building certain IT systems.

CDT Should Urgently Assess the State's Information Security Status

CDT has asserted that knowing the State's current information security status is necessary in order to implement effective improvements. However, CDT does not have a comprehensive knowledge of the status of statewide information security. To help protect the State from cybersecurity risks, CDT should urgently develop a plan for more quickly assessing the reporting entities' information security status. This plan might include increasing the number of its staff who are available to perform compliance audits or revising its review process to allow it to more quickly understand each reporting entity's information security status. The plan might also involve pursuing enforcement measures and corrective actions for agencies that do not address security deficiencies, such as requiring reporting entities to address outstanding information security deficiencies before implementing new IT initiatives.

CDT has yet to implement our January 2022 recommendation that it increase its capacity to perform timely compliance audits of high-risk reporting entities. It asserted that it is exploring different strategies to more quickly establish the status of information security statewide; however, each of its possible solutions is still in preliminary stages of development.

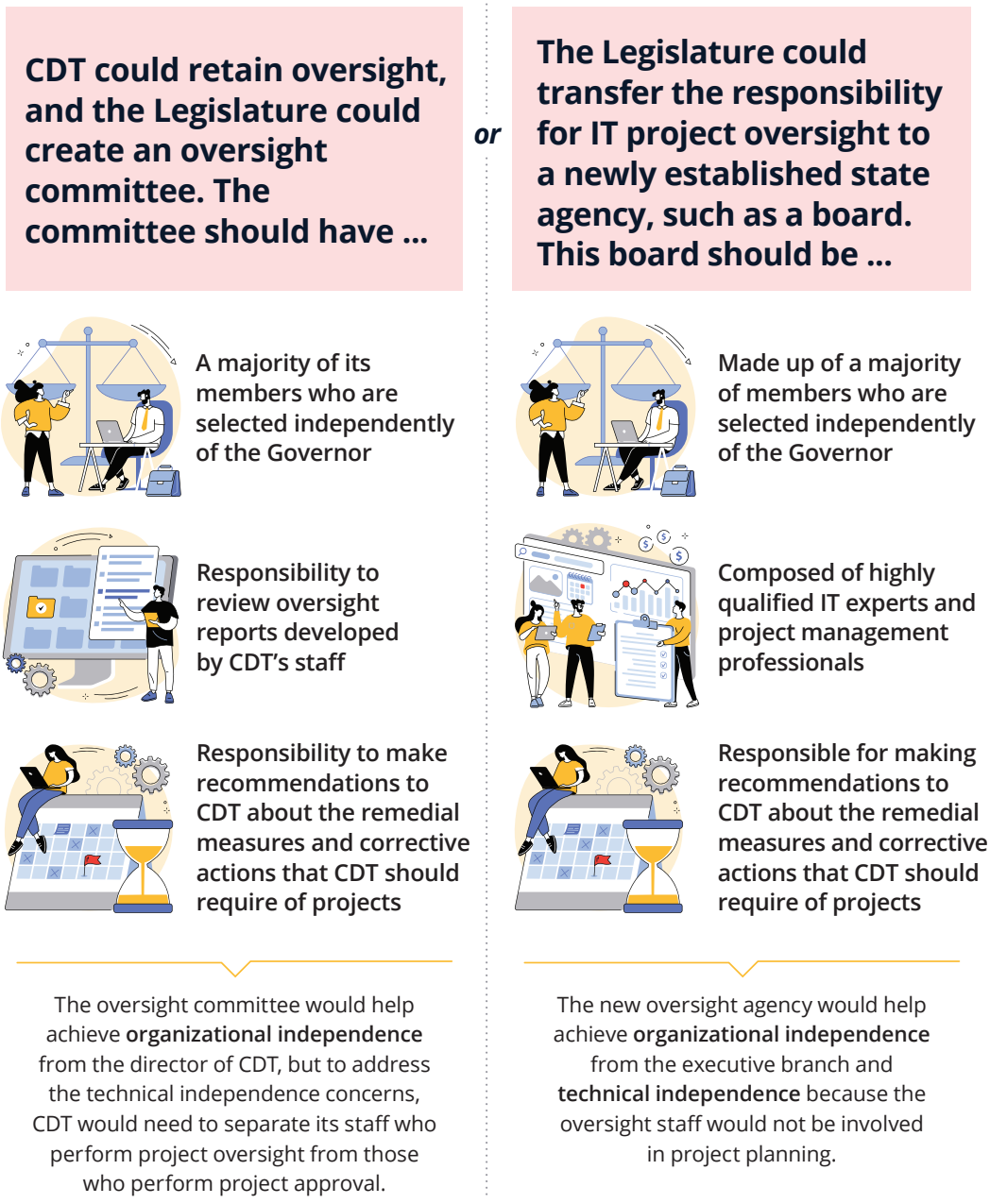
The Legislature Should Make Changes to Improve the Independence of IT Project Oversight

CDT's inability to implement adequate measures to ensure the objectivity of its project oversight and to improve the effectiveness of that oversight raises concerns about its willingness to suspend or curtail projects that exceed their planned schedule or cost. As a result, we believe that the Legislature should consider making changes to ensure that IT project oversight is performed by an independent state agency or entity, as Figure 10 shows, and that has reporting responsibility to the Legislature.

The Legislature could consider several alternatives for establishing such an agency or entity. One approach would be to create a new state agency, such as a board with IT project oversight responsibilities that reports to the Legislature. If the Legislature takes this approach, the new oversight agency should be staffed with highly qualified IT experts and IT project management professionals. A majority of the board members should be selected independently of the Governor by, for example, leaders

of the Legislature. The board members could include representatives from state agencies, the Legislature, and the private sector. The board members should be responsible for selecting the individual who would directly manage the oversight staff.

Figure 10
The Legislature Should Consider Making Changes to Ensure That Project Oversight Is Independent



Source: Analysis of state law, *State Administrative Manual*, Institute of Internal Auditors, and best practices from other states.

The Legislature should task the new oversight board with oversight of IT projects that includes, but is not limited to, substantive tracking, measurement, and analysis of a project's progress against the original approved project plan as well as against any approved changes to the plan. The board should also be responsible for making recommendations to CDT for how to enforce compliance with approved project objectives, how to require state agencies to address issues that impair a project's ability to meet those objectives in a timely, cost-effective manner, and when to suspend or terminate a project. This type of oversight board would have organizational independence from the executive branch and would have technical independence because the oversight staff would not be involved in project planning.

Alternatively, CDT could continue to perform its oversight responsibilities, but the Legislature could create a committee that would review CDT's oversight reports. If the Legislature takes this approach, CDT's oversight manager should report to the committee in addition to CDT's directorate. The selection and composition of committee members and the recommendations the committee would be tasked with making to CDT would be similar to those of the board we describe above. Although an oversight committee of this nature would help improve organizational independence from the director of CDT, CDT would need to address the technical independence concerns by separating its staff who perform project oversight from those who perform project approval. Because the purpose of oversight is to provide an independent review and analysis of the project's progress, either the board or the committee approach would improve independence by helping to ensure that objective information is communicated to decision makers such as CDT and the Legislature and would increase the likelihood that they will take appropriate action in response to the oversight findings.

RECOMMENDATIONS

Legislature

The Legislature should revise state law to clarify CDT's role, responsibilities, and priorities for strategically guiding the State's acquisition, management, and use of IT. The revised priorities should require CDT to do the following:

- Follow best practices in its 2024 strategic plan and all future strategic plans by developing measurable objectives to achieve goals and incorporating performance measures for those objectives. Further, it should pursue accountability by monitoring the State's progress toward achieving the plan's goals.

- Develop a plan by July 1, 2023, for satisfying its statutory requirement to identify, assess, and prioritize modernizing high-risk, critical IT systems.

- By March 2024, develop and maintain an inventory of the State's IT systems or components of systems that agencies can reuse to avoid duplication of efforts.

The Legislature should require CDT to create and lead an interorganizational task force to assess IT staffing problems in the State and to issue recommendations to increase the State's hiring and retention rates of highly qualified IT personnel. The task force should be composed of CDT staff, state IT staff, and state human resources staff.

The Legislature should require CDT to develop a plan for determining the overall statewide information security status of the State's reporting entities by January 2024. This plan may entail CDT's assessing reporting entities through its existing oversight lifecycle or through alternative processes. It may include increasing the number of CDT staff, revising CDT's review process, or pursuing enforcement measures and corrective actions for reporting entities that do not address information security deficiencies. For example, when appropriate, CDT could require reporting entities to address outstanding information security deficiencies before implementing new IT initiatives.

The Legislature should make changes to improve the independence of the State's IT project oversight. One option it could consider is creating a new state entity, such as an independent board, that is specifically tasked with certain oversight responsibilities for IT projects. If the Legislature pursues this option, the majority of the board members should be selected independently of the Governor by, for example, leaders of the Legislature or other elected state officers. The board could include representatives from state agencies, the Legislature, and the private sector. Alternatively, CDT could continue to perform its oversight responsibilities and the Legislature could create a committee to review CDT's oversight reports. The new board or committee should be tasked with making recommendations to CDT about the remedial measures and corrective actions that CDT should require of the agency performing the project to resolve problems in a timely manner, as well as recommendations about suspending, reinstating, and terminating IT projects. The new oversight board or committee should report regularly to the Legislature and project stakeholders on each project's progress in meeting its approved objectives.

If it decides to create a new oversight board or committee, the Legislature should ensure that board or committee's ability to provide effective oversight by requiring it to do the following:

- Include, in the project oversight reports, substantive analyses of the key indicators of a project's progress—such as schedule, scope, cost, and staffing resources—that are based on the original approved project plan. The oversight reports should also identify any changes made to the project plan by a special project report, a contract amendment, or department change orders.

- Establish a knowledge group composed of IT industry experts, CDT staff, agency information officers and chief information officers, and state policymakers to establish clear, data-driven guidelines and metrics for suspending, reinstating, and terminating IT projects to decrease the frequency and severity of IT system failures, cost overruns, delayed implementation, and limited functionality. The knowledge group should base the guidelines on industry best practices for determining IT project success.

- Periodically analyze the lessons learned that are included in agencies' post implementation evaluation reports to identify trends or patterns. The new oversight board or committee should also require state agencies to complete post implementation evaluation reports for projects that are terminated before implementation. The board or committee should use the information from both types of reports to improve its oversight processes.

CDT

To ensure that it consistently applies best practices when conducting strategic planning, CDT should develop a policy or procedure that documents the required elements of its strategic plan. These elements should include key goals, strategies for achieving those goals, measurable objectives, performance measures, and processes to monitor progress.

To expand its knowledge of threats to the State's information security and more effectively leverage the State's resources for threat monitoring, CDT should perform increased outreach with reporting entities. Specifically, CDT should learn what reporting entities are currently doing for monitoring and alerting other agencies of cybersecurity threats and educate them about its no-cost threat monitoring service.

To improve the effectiveness of the PAL process at ensuring the success of projects, CDT should take the following actions:

- Revise the PAL process to promote the use of modern approaches, such as modular or agile, when developing new systems. Further, CDT should maintain awareness of new development approaches and update its approval process to encourage their use, whenever feasible.

- Revise the PAL process to require agencies to ensure, and CDT to verify, that proposed projects align with statewide strategic initiatives so that all approved projects are contributing to the State's strategic goals.

- Develop internal metrics that include information on each project's size, the timeliness with which a solution was procured, the length of time to complete each stage of PAL, the degree to which an implementation was successful, and the degree to which the project was completed on time and within budget. CDT should trend the results of these internal metrics over time and include them in its annual report to the Legislature.

We conducted this performance audit in accordance with generally accepted government auditing standards and under the authority vested in the California State Auditor by Government Code section 8543 et seq. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on the audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Respectfully submitted,

GRANT PARKS
California State Auditor

April 20, 2023

Staff:	Nicholas Kolitsos, CPA, Audit Principal Jordan Wright, CFE Trunice Anaman-Ikyurav Salma Healy David A. Monnat, CPA, MAcc Alya Proshak
Data Analytics:	Sarah Rachael Black, MBA, CISA Kim Buchanan, MBA, CISA
Legal Counsel:	Joe Porche

Appendix A

Survey Information

We conducted an online survey of all state agencies to determine the extent to which they are aware of, using, and satisfied with the services CDT provides. We sent the survey to the agency information officers and chief information officers and related representatives of 143 state agencies and received a total of 103 responses. We asked the agencies to rate and describe their experiences with CDT's services, to provide information related to CDT's information security services, and to provide information about IT systems that they believe need to be modernized. We used the responses from the survey to support findings and conclusions throughout this report. We provide information related to the survey in the following table and figures.

Table A
State Agencies That Did Not Respond to Our Survey

	STATE AGENCY (IN ALPHABETICAL ORDER)
1	Air Resources Board, California
2	Alcoholic Beverage Control, California Department of
3	Arts Council, California
4	Asian and Pacific Islander American Affairs, California Commission on
5	Cannabis Control Appeals Panel
6	Citizens Compensation Commission, California
7	Coastal Commission, California
8	Colorado River Board of California
9	Community Services and Development, California Department of
10	Compensation Insurance Fund, State
11	Cradle-to-Career, California System
12	Data and Innovation, Office of
13	Delta Protection Commission
14	Delta Stewardship Council
15	Developmental Disabilities, California State Council on
16	Energy Commission, California
17	Energy Infrastructure Safety, Office of
18	Fish and Wildlife, California Department of
19	General Services, California Department of

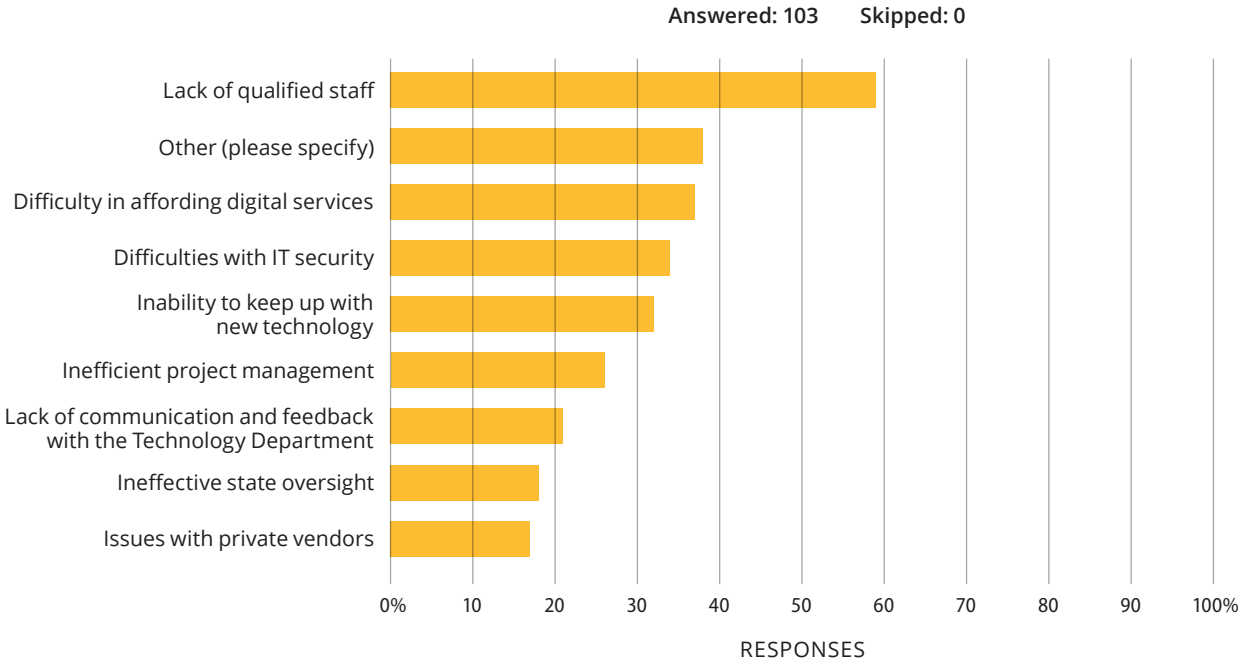
continued on next page . . .

	STATE AGENCY (IN ALPHABETICAL ORDER)
20	Health Benefit Exchange, California
21	Homelessness, California Interagency Council on
22	Housing and Community Development, California Department of
23	Independent Living Council, California State
24	Law Revision Commission, California
25	Native American Heritage Commission
26	Natural Resources Agency, California
27	Patient Advocate, Office of the
28	Peace Officer Standards and Training, Commission on
29	Personnel Board, California State
30	Prison Industries Authority, California
31	Privacy Protection Agency, California
32	Public Employment Relations Board
33	Rehabilitation, Department of
34	Resources Recycling and Recovery, California Department of
35	San Gabriel & Lower Los Angeles Rivers and Mountains Conservancy
36	Secretary of State, California
37	Seismic Safety Commission, Alfred E. Alquist
38	State and Community Corrections, Board of
39	Status of Women and Girls, California Commission on the
40	Summer School for the Arts, California State

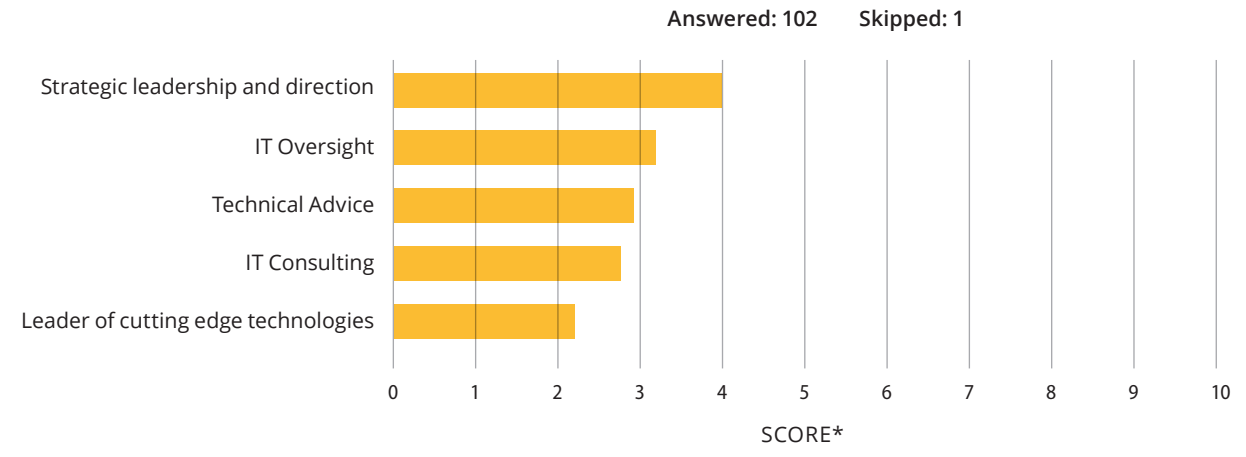
Source: State Auditor's IT services survey.

Figure A1
Aggregated Survey Responses Related to Agencies' Use of and Satisfaction With CDT's Services

What are the most significant IT challenges your organization is encountering? Please select all that apply.



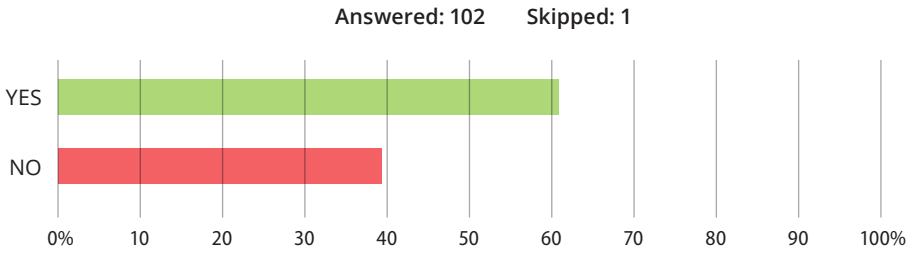
From your organization's perspective, please rank the provided roles below in the order of importance, with the top position being the Technology Department's main role.



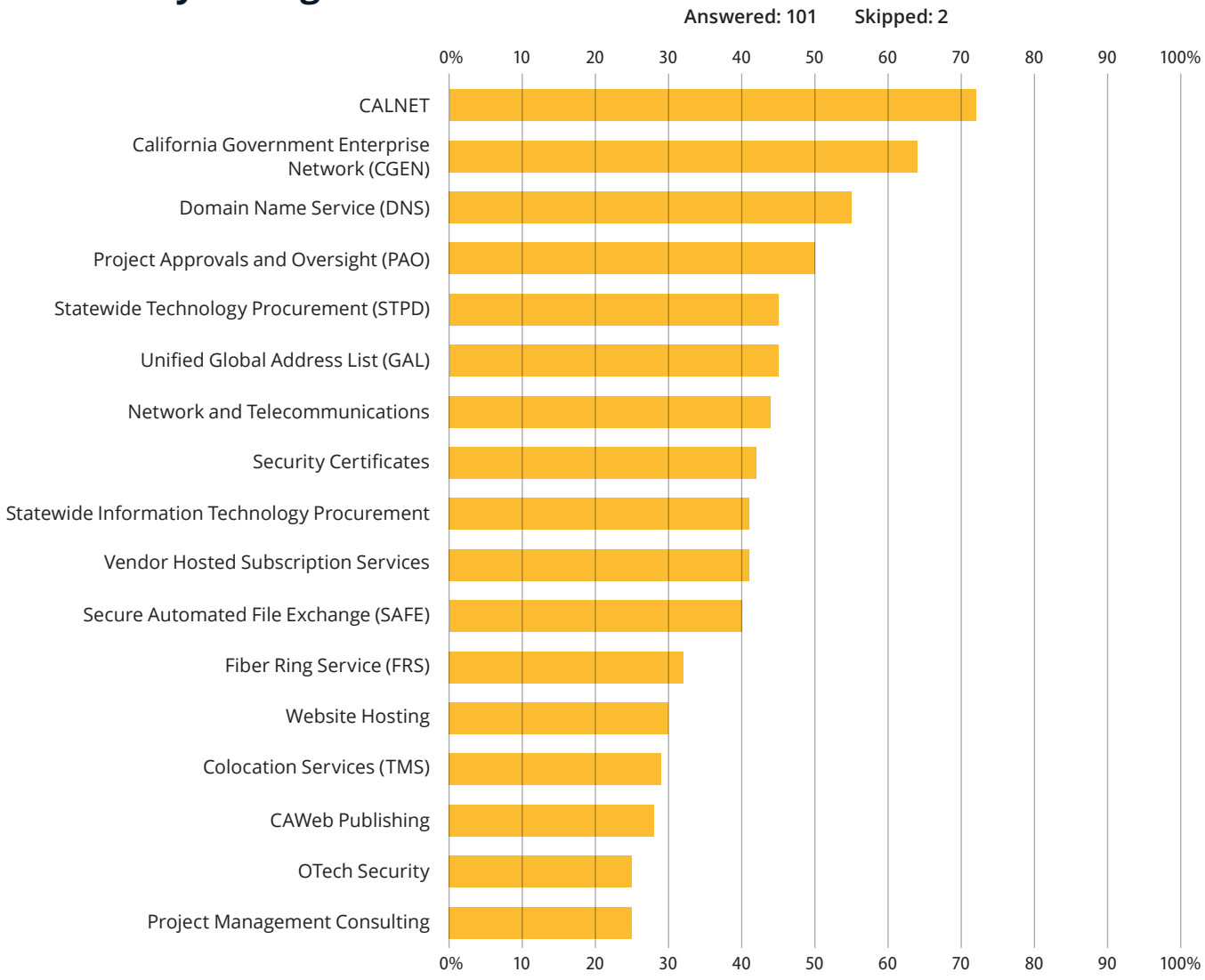
* The score is based on the ranking and number of departments. A higher score indicates higher perceived importance of that role.

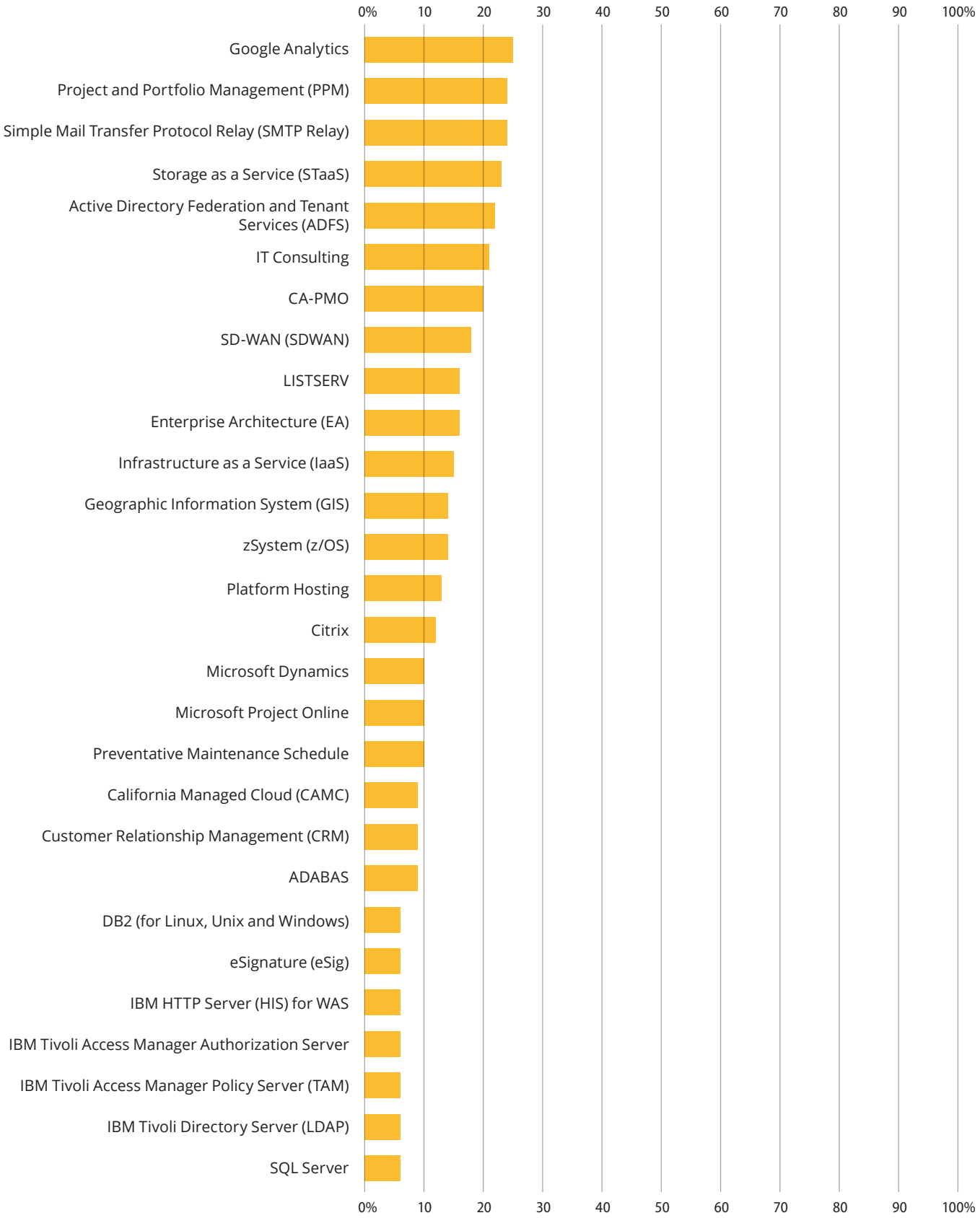
continued on next page . . .

Do you believe the Technology Department adequately fulfills its main role?

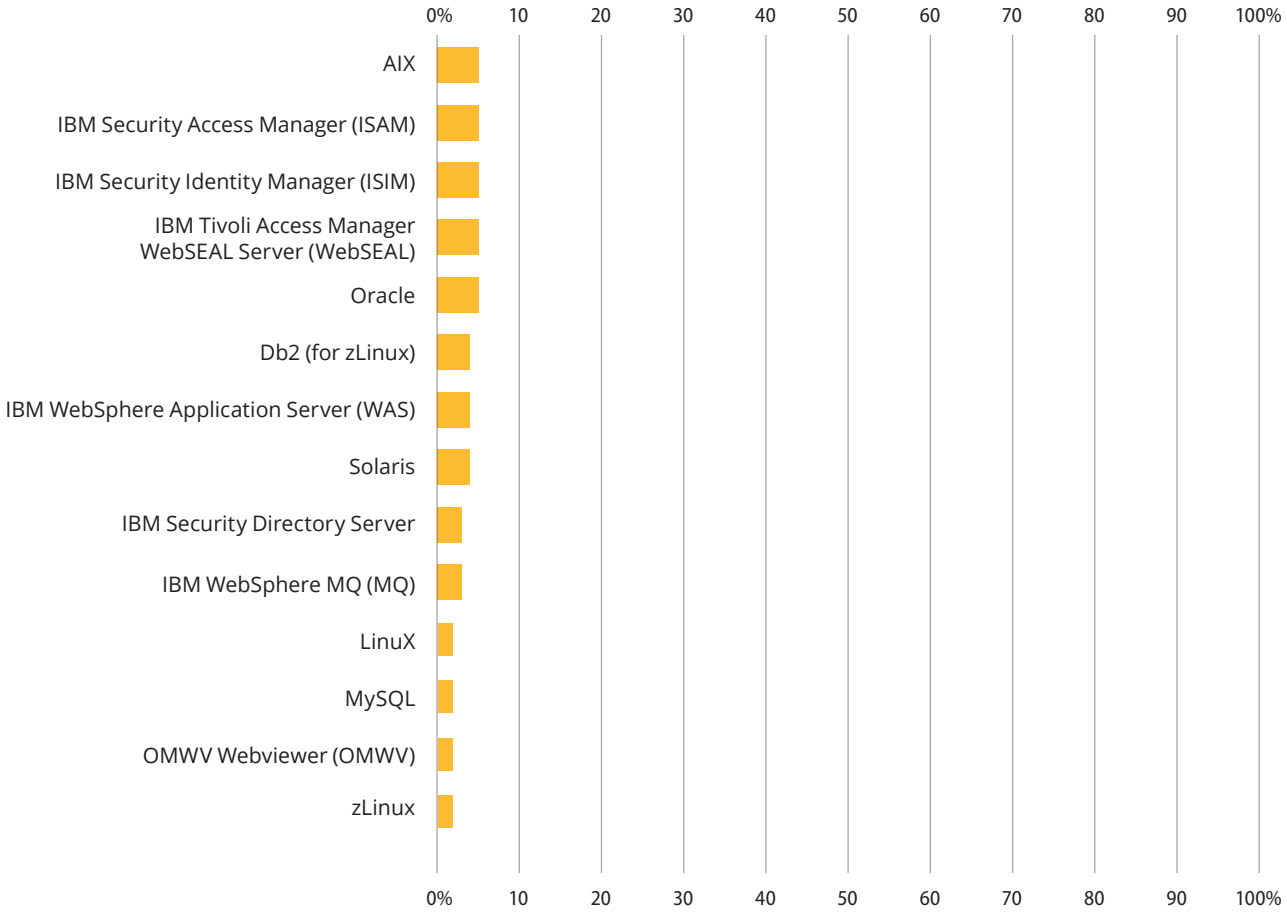


Please select the Technology Department-provided services that your organization uses.

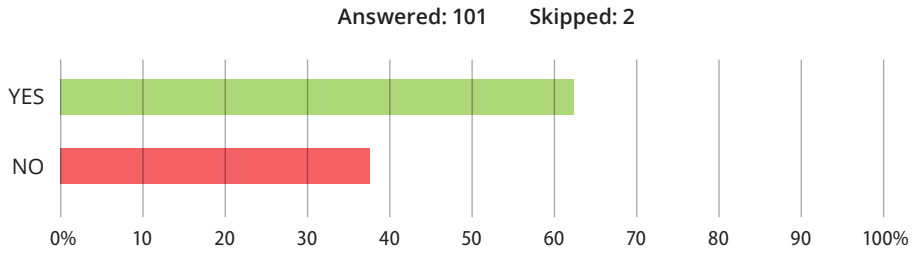




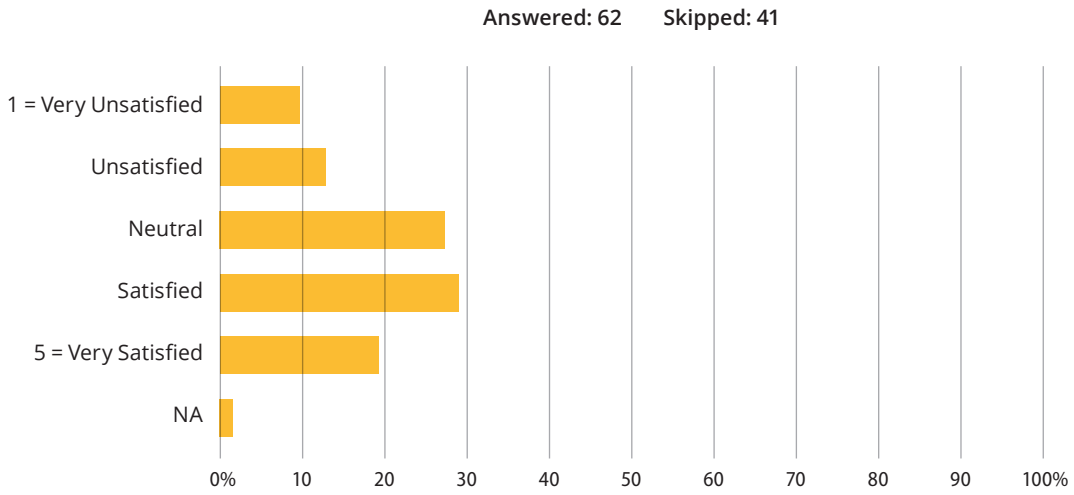
continued on next page . . .


0%
10
20
30
40
50
60
70
80
90
100%
AIX
IBM Security Access Manager (ISAM)
IBM Security Identity Manager (ISIM)
IBM Tivoli Access Manager WebSEAL Server (WebSEAL)
Oracle
Db2 (for zLinux)
IBM WebSphere Application Server (WAS)
Solaris
IBM Security Directory Server
IBM WebSphere MQ (MQ)
LinuX
MySQL
OMWV Webviewer (OMWV)
zLinux

Has your organization ever used the Technology Department's project approval services?

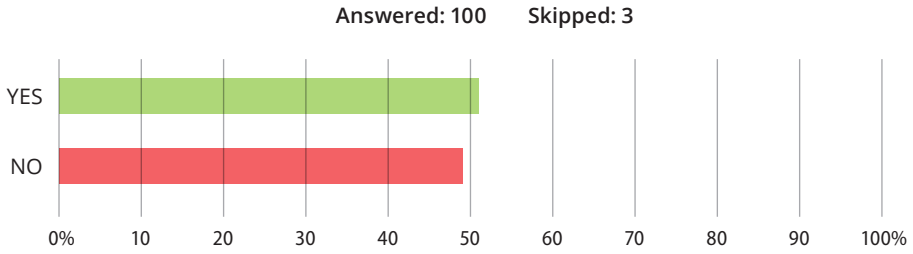


On a scale from 1 to 5, with 1 = Very Unsatisfied and 5 = Very Satisfied, how would you rate your satisfaction with the project approval service by the Technology Department?

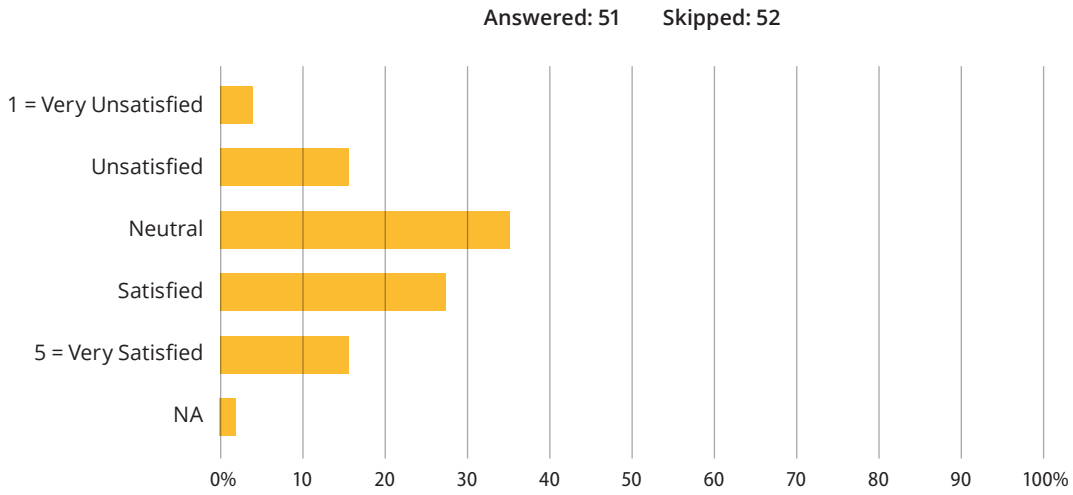


continued on next page . . .

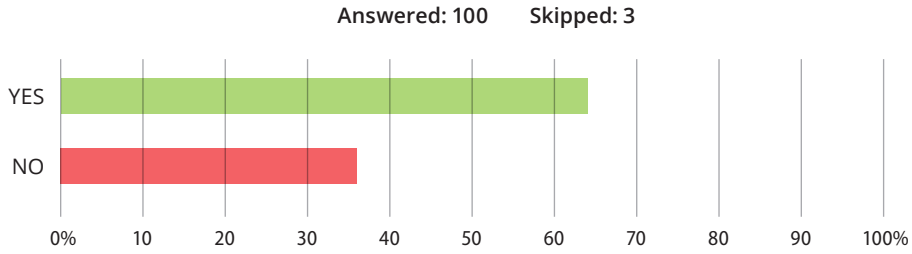
Has your organization ever used the Technology Department's project oversight services?



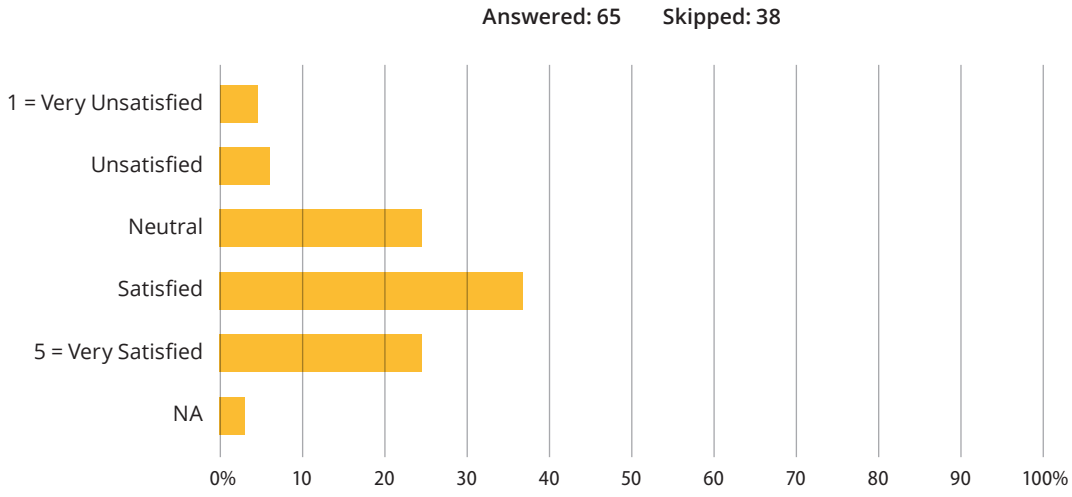
On a scale from 1 to 5, with 1 = Very Unsatisfied and 5 = Very Satisfied, how would you rate your satisfaction with the project oversight service by the Technology Department?



Has your organization ever used the Technology Department's technology procurement services?

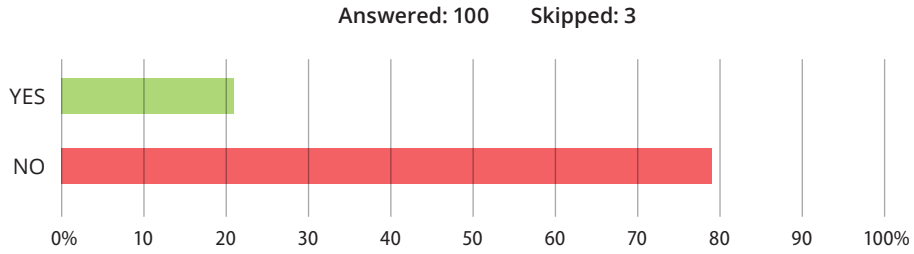


On a scale from 1 to 5, with 1 = Very Unsatisfied and 5 = Very Satisfied, how would you rate your satisfaction with the technology procurement service by the Technology Department?



continued on next page . . .

Has your organization ever used the Technology Department's IT consulting service?



On a scale from 1 to 5, with 1 = Very Unsatisfied and 5 = Very Satisfied, how would you rate your satisfaction with the IT consulting service by the Technology Department?

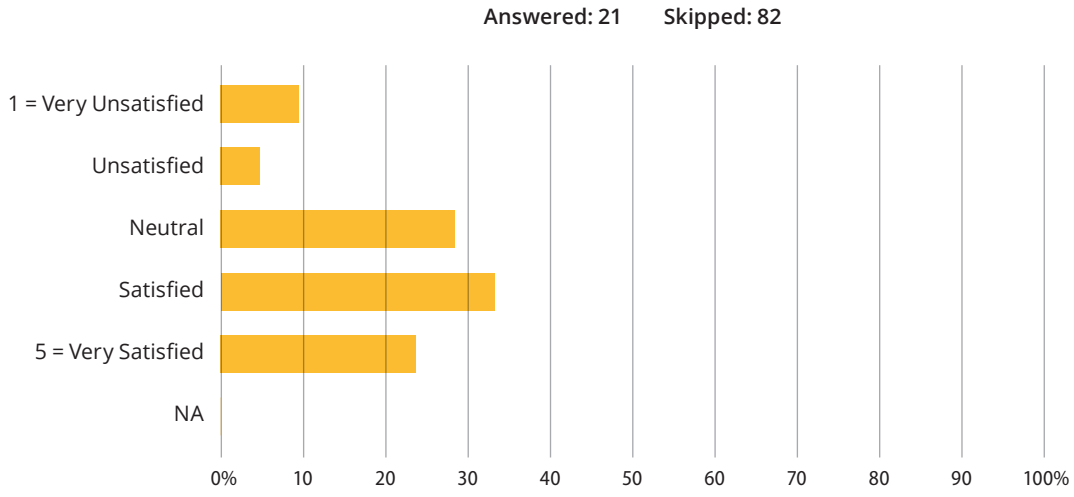
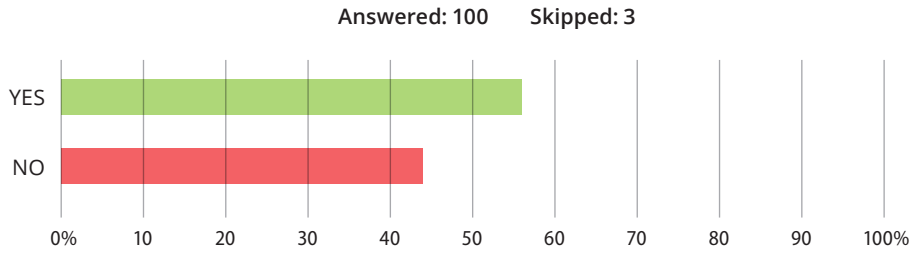
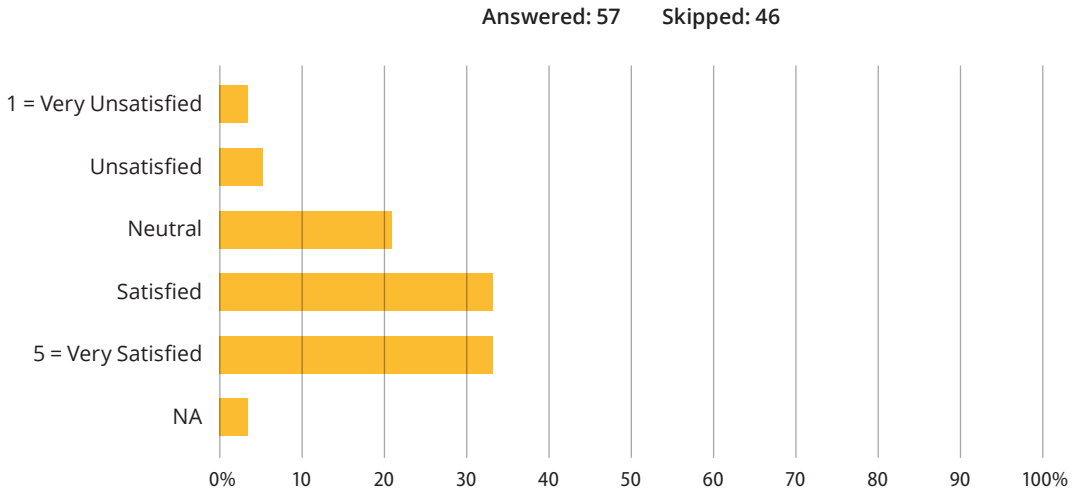


Figure A2
Aggregated Survey Responses Related to Information Security

Has your organization ever used the Technology Department's information security services?

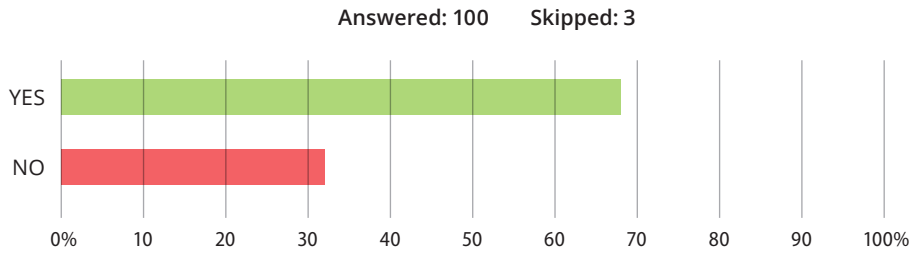


On a scale from 1 to 5, with 1 = Very Unsatisfied and 5 = Very Satisfied, how would you rate your satisfaction with the information security service by the Technology Department?

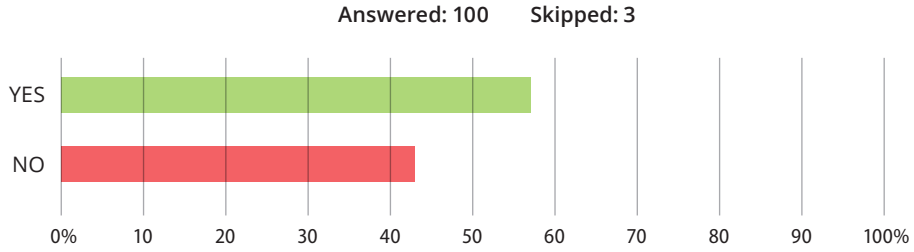


continued on next page . . .

The Technology Department offers continuous monitoring for detection of cyber threats and sends out alerts to notify state departments of any suspicious activity that is detected. Were you aware that the Technology Department offered this service?



Were you aware that there is currently no cost to state departments to participate in CDT's cyber threat monitoring?



Do you currently participate in CDT's cyber threat monitoring?

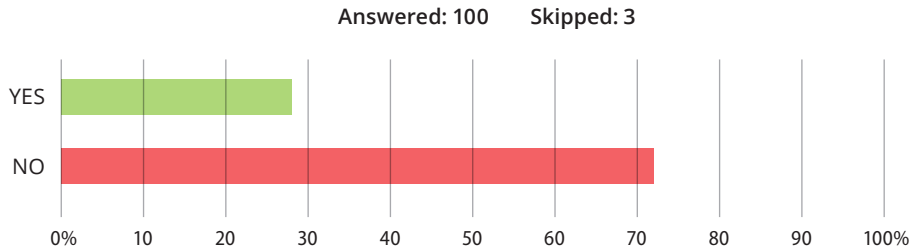
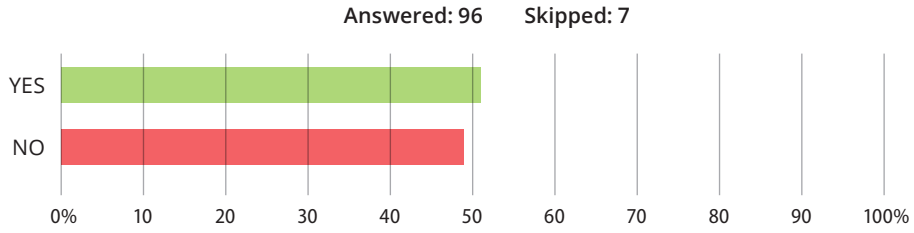
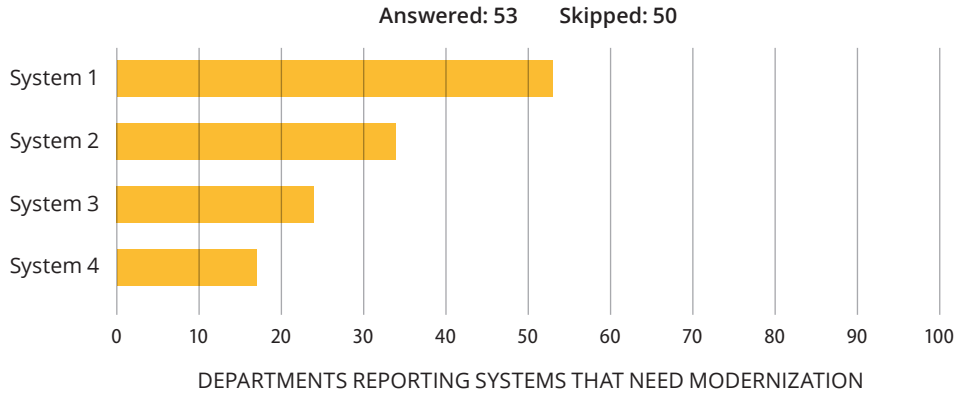


Figure A3
Aggregated Survey Responses Related to IT Systems That Need to Be Modernized

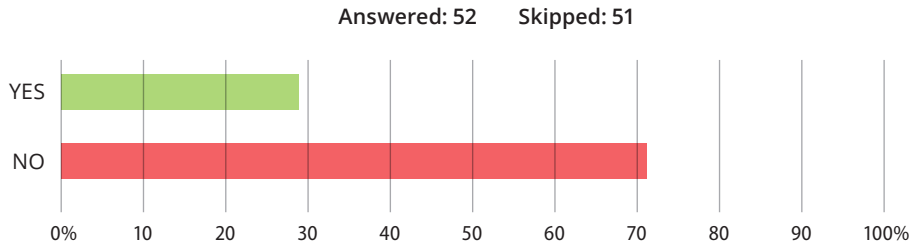
Do you have any information technology systems that you believe need to be modernized?



Please provide up to four of the most important systems your department operates that need modernization and describe why they need to be modernized.



For the systems that need to be modernized, do you have any documented modernization plans?



Blank page inserted for reproduction purposes only.

Appendix B

Contracts and Amendments of the IT Projects We Reviewed

Table B presents key information for contracts and amendments of the IT projects we reviewed, including the vendor, amount, term, and reason for the contract or amendment. Table B also includes specific details of instances when the contract's budget was increased or the schedule was extended.

Table B
Contracts and Amendments for IT Projects We Reviewed

CONTRACT NUMBER AND VENDOR	MAXIMUM CONTRACT AMOUNT	TERM	KEY REASON FOR CONTRACT OR AMENDMENT	CHANGE TO BUDGET OR SCHEDULE
IT Project: FI$Cal				
FI$Cal 021-11—Accenture, LLP Original contract (1 of 2) Approved June 14, 2012	$198,288,434	June 18, 2012 through August 21, 2017	Design, development, implementation, and maintenance of an enterprise resource planning system that will be called FI$Cal	NA
Amendment 1— Approved August 13, 2013	198,288,434	June 18, 2012 through August 21, 2017	Moved funding from one year to another	NA
Amendment 2— Approved December 16, 2013	212,074,998	June 18, 2012 through August 21, 2017	Contract amount increase, added operations and maintenance to scope	$13,786,564
Amendment 3— Approved April 7, 2014	225,986,320	June 18, 2012 through August 21, 2018	Contract amount increase, change to implementation approach, schedule extension	13,911,322 added 1 year
Amendment 4— Approved December 8, 2015	236,746,267	June 18, 2012 through August 21, 2018	Contract amount increase, additional scope for an enhanced vendor portal and unanticipated tasks	10,759,947
Amendment 5— Approved July 8, 2016	298,236,267	June 18, 2012 through June 30, 2019	Contract amount increase, schedule extension	61,490,000 added approximately 10 months
Amendment 6— Approved November 7, 2017	303,236,267	June 18, 2012 through June 30, 2019	Contract amount increase for unanticipated tasks	5,000,000
Amendment 7— Approved February 6, 2018	319,704,237	June 18, 2012 through June 30, 2019	Contract amount increase for SCO/STO sprint periods	16,467,970
Amendment 8— Approved October 31, 2018	327,682,018	June 18, 2012 through October 31, 2019	Contract amount increase for enterprise resource planning support periods	7,977,781 added 4 months
Amendment 9— Approved June 27, 2019	376,080,844	June 18, 2012 through June 30, 2022	Contract amount increase, additional scope for supplemental services and unanticipated tasks, schedule extension	48,398,826 added 32 months

continued on next page . . .

CONTRACT NUMBER AND VENDOR	MAXIMUM CONTRACT AMOUNT	TERM	KEY REASON FOR CONTRACT OR AMENDMENT	CHANGE TO BUDGET OR SCHEDULE
FI$Cal 024-11 Accenture, LLP Original Contract (2 of 2) Approved June 14, 2012	$13,786,564	June 18, 2012 through August 21, 2017	Design, development, implementation, operation, and maintenance of an enterprise resource planning system that will be called FI$Cal	NA
Amendment 1— Approved August 13, 2013	13,786,564	June 18, 2012 through August 21, 2017	Statement of work change to reconcile language with and include changes from FI$Cal 021-11 amendment 1	NA
Amendment 2— Approved December 17, 2013	0 (zero)	Effective December 17, 2013	Terminated the contract. Moved funding and maintenance and operations scope to FI$Cal 021-11 amendment 2 above	($13,786,564)
FI$Cal 013-12— International Business Machines (IBM) Corporation Original Contract Approved October 10, 2012	3,269,504	October 8, 2012 through June 30, 2016	Enterprise Resource Planning Advisory Services	NA
FI$Cal 008-13— CherryRoad Technologies Inc. Original Contract Approved August 19, 2013	25,930,000	June 28, 2013 through June 30, 2017	Legacy Systems and Services expertise and services	NA
Amendment 1— Approved July 11, 2014	25,930,000	June 28, 2013 through June 30, 2017	Statement of Work change to require live scan background checks	NA
Amendment 2— Approved February 26, 2015	25,930,000	June 28, 2013 through June 30, 2017	Statement of Work change	NA
Amendment 3— Approved June 12, 2017	25,930,000	June 28, 2013 through June 30, 2018	Schedule extension, Statement of Work change	added 1 year
IT Project: Child Welfare System*				
75334059—KPMG LLP Original Contract— Approved February 28, 2021	$13,073,280	March 1, 2021 through February 29, 2024	Product Value Services, such as research and service design	NA
Amendment 1— Approved January 20, 2023	26,931,840	March 1, 2021 through February 28, 2027	Contract amount increase, schedule extension, Statement of Work change	$13,858,560 added 3 years
75334060—Deloitte Consulting LLP Original Contract— Approved April 1, 2021	48,920,927	April 1, 2021 through March 31, 2024	Platform as a Service Systems Integrator	NA
75334061—OnCore Consulting, LLC Original Contract— Approved April 15, 2021	33,218,581	April 15, 2021 through April 14, 2024	CARES Data Infrastructure Services	NA
75334086—Deloitte Consulting LLP Original Contract— Approved July 7, 2021	26,295,829	July 7, 2021 through July 6, 2024	Implementation Services	NA

CONTRACT NUMBER AND VENDOR	MAXIMUM CONTRACT AMOUNT	TERM	KEY REASON FOR CONTRACT OR AMENDMENT	CHANGE TO BUDGET OR SCHEDULE
75334140— Business Advantage Consulting, Inc. Original Contract— Approved August 23, 2021	$6,234,880	September 1, 2021 through August 31, 2024	Quality Assurance Testing Services	NA
IT Project: DMV-Digital Experience Platform				
TC21-014—Deloitte Consulting, LLP Original Contract— Approved September 10, 2021	$7,085,900	September 10, 2021 through September 13, 2023	Occupational Licensing System Integration	NA
Amendment 1— Approved September 26, 2022	7,794,490	September 10, 2021 through September 13, 2023	Contract amount increase for unanticipated tasks	$708,590
TC22-010—Deloitte Consulting, LLP Original Contract— Approved August 30, 2022	46,684,198	August 30, 2022 through February 28, 2025 with 5 options to extend 6 months	Design, development, and implementation services and maintenance and operations services	NA
IT Project: DOT-Transportation Asset Management System				
56A0651—Data Transfer Solutions, LLC Original Contract— Approved February 23, 2021	$15,462,308	February 23, 2021 through February 21, 2024	Implementation of a Transportation Asset Management System	NA
Amendment 1— Approved June 2, 2021	15,462,308	February 23, 2021 through February 21, 2024	Added license agreement	NA
Amendment 2— Approved June 28, 2022	15,462,308	February 23, 2021 through February 21, 2024	Reduction of scope and costs related to licenses	"amount of this agreement is reduced by the value of all licenses"
Stop Work Order— Issued April 29, 2022 Amendment 2 Exhibit A	NA	April 29, 2022 through August 12,2022	Order requiring vendor to stop all development work related to implementation of outstanding deliverables	NA
Amendment 3— Approved August 26, 2022	35,000	Term reduced to end on August 26, 2022	Settlement Agreement and termination of contract	$35,000 payable by Caltrans under the settlement agreement

Source: IT project contracts and amendments.

NA = Not applicable.

* After it was first approved, the Child Welfare System project changed its development approach to a modular/agile approach using open-source coding. During the open-source coding approach, the project did not have a prime vendor but had partnered with the Office of Systems Integration to perform initial planning, procurement, and design and development work and act as the system integrator. The project subsequently pivoted to its current modular/agile approach using Salesforce as the low-code platform and Deloitte as the system integrator.

Blank page inserted for reproduction purposes only.

Appendix C

Scope and Methodology

The Joint Legislative Audit Committee (Audit Committee) directed the California State Auditor's Office to conduct an audit of CDT to provide independently developed information related to CDT's oversight of state IT projects and the State's safeguards against cybersecurity threats. We reviewed CDT's project oversight, its procurements for a selection of IT projects, and its leadership of the State's cybersecurity efforts. Table C lists the objectives that the Audit Committee approved and the methods we used to address them.

Table C
Audit Objectives and the Methods Used to Address Them

	AUDIT OBJECTIVE	METHOD
1	Review and evaluate the laws, rules, and regulations significant to the audit objectives.	Reviewed relevant laws, rules, regulations, policies, and procedures related to CDT and state IT project oversight and the State's cybersecurity.
2	Review and evaluate the processes used by CDT for reviewing and approving IT procurements and determine the degree to which CDT is responsible for statewide oversight, coordination, planning, and leadership, as well as the effective uses of IT, including new systems that would allow for interdepartmental communication and information sharing.	• Interviewed CDT's procurement staff and assessed its PAL review and approval process for effectiveness. • Reviewed three projects that were approved through the PAL process to ensure compliance with key requirements. • Interviewed CDT staff; reviewed state law, policies, and strategic plans; and determined the degree of CDT's statutory responsibility for statewide oversight, coordination, planning, leadership, and effective use of IT. • Reviewed state law and administrative manuals and conducted Internet research to identify state agencies other than CDT with IT responsibilities. • Reviewed the public websites of the additional state agencies we identified to determine whether their missions, authority, or responsibilities appear to overlap with, represent gaps in, or misalign with CDT's scope of responsibility.
3	Review and evaluate the level of oversight CDT provides on statewide IT and security, including but not limited to determining the following:	
	a. Whether CDT has conducted an inventory of all the IT systems used by agencies throughout the State, including the age of the systems and the adequacy of their security controls.	• Interviewed key CDT staff to determine whether CDT has conducted an inventory of all IT systems. • Reviewed relevant CDT documentation, such as memoranda, surveys, and assessment reports that pertain to its stabilization service.
	b. Whether CDT has identified all the legacy systems in need of modernization, including those that have unsupported hardware and software, are using outdated languages, or are operating with known security vulnerabilities.	• Interviewed CDT staff and analyzed CDT's draft plans to understand its progress in identifying systems in need of modernization. • Included questions about systems in need of modernization in our survey, which we describe in Objective 7.
	c. Whether CDT is involved in making key decisions, including the development of modernization plans, and ensuring that the systems meet the needs of agencies.	Reviewed the documented modernization plans that state agencies submitted as part of our survey to evaluate the role CDT has when a system undergoes modernization under the PAL review process.

continued on next page . . .

	AUDIT OBJECTIVE	METHOD
	d. The extent to which CDT has assessed and measured the information security status across the State.	• Interviewed CDT staff and analyzed relevant documents to understand how CDT plans to implement its current four-year oversight lifecycle. • Assessed CDT's current audit schedule to determine how many reporting entities it plans to review and whether that number will be sufficient to establish the State's information security status in a timely manner. We did not look at nonreporting entities for this audit because they are not required to follow CDT's information security policies and procedures. Our January 2022 report provides more detail about the information security status of nonreporting entities.
	e. The extent to which CDT has monitored potential or actual security threats across the State.	• Identified CDT's partners for sharing of threat intelligence and determined how CDT leverages these relationships to identify threats to the State's information security. • Determined how many state entities use CDT's threat monitoring service and interviewed CDT staff to learn why it does not require that all reporting entities submit their logs for review.
4	Review CDT's role in managing a selection of procurements of IT and whether it routinely followed laws, rules, regulations, policies, and best practices when selecting vendors for the system including, to the extent possible, those prohibiting a conflict of interest during the selection process.	• Selected the following four IT procurements for review based on factors such as cost, procuring agency, and contract length: Franchise Tax Board's Enterprise Data to Revenue Phase 2 project; California Department of Food and Agriculture's Cannabis Activity Tracking project; California Department of Public Health's Management Information System for California's Special Supplemental Nutrition Program for Women, Infants and Children; and California Department of Veterans Affairs' Electronic Health Records project. • Reviewed the procurements to determine the effectiveness of CDT's IT project procurement management and its compliance with requirements in state law and policy, including rules regarding conflicts of interest.
5	Review a selection of IT projects at state agencies for which CDT provides services, including recent projects at EDD and FI$Cal, and determine whether CDT fulfilled its roles and responsibilities. Specifically, perform the following: a. Identify the estimated and actual implementation costs and timelines for the system, as well as the number of and reasons for change orders and contract amendments.	• Selected four IT projects at state agencies for which CDT provides services, which are listed in Table 2. • Worked with an IT consultant to review project oversight reports and other project documentation. Because CDT does not review or approve change orders, we focused our review on CDT's monitoring of contract amendments and its independent project oversight of projects' costs, scopes, and schedules. We present the number of and reasons for contracts and amendments in Appendix B. • Reviewed EDD's recent modernization project to identify the key causes for restarting it. We interviewed CDT staff and reviewed PAL documentation and the EDD Strike Team report. • Reviewed our past FI$Cal reports and compiled the key findings and recommendations to identify the root causes of the system's ongoing problems, delays, and increasing costs. • Compiled the main findings from our past audit reports regarding CDT and analyzed them to identify key weaknesses and their causes.
	b. Determine whether the original project requirements, as defined by the scopes of work, were delivered in a timely manner during implementation of the system projects.	Reviewed CDT's project oversight reports to determine whether project requirements were delivered in a timely manner during project implementation.
	c. Evaluate the steps CDT took when project variances were identified within its scope of responsibility. To the extent possible, determine whether CDT could have identified problems with the systems earlier.	Assessed CDT's project oversight process and reviewed its project oversight reports, escalation documents, and special project reports.

	AUDIT OBJECTIVE	METHOD
	d. If applicable, determine whether the agencies and/or CDT have documented lessons learned for use in future phases of system implementations.	Determined whether the state agencies or CDT have documented lessons learned as required by policy and have used them in future phases of system implementations.
6	Determine whether CDT is the right size to appropriately perform its statutory responsibility to oversee IT project development and IT security, including whether additional qualified staff would meaningfully improve its services with respect to information security and IT projects.	• Reviewed CDT's vacancy reports to identify unaddressed staffing needs. • Reviewed CDT's budget change proposals for fiscal years 2017–18 through 2022–23 to identify any staffing needs. • Interviewed CDT staff, reviewed a list of CDT's contracted consultants, and assessed a selection of contracts to determine whether consultants and contracted employees are providing services to CDT in lieu of department staff. We did not identify any issues related to CDT's use of contracted consultants. • Interviewed CDT staff and evaluated relevant documentation to assess the adequacy of CDT's plan for increasing its capacity to perform timely compliance audits.
7	Conduct a survey of all state agencies within CDT's scope of responsibility to assess the extent to which they are aware of, using, and satisfied with the services that CDT offers, including project approvals and oversight, technology procurement, IT consulting, and information security.	• Identified all applicable state agencies and their chief information officer or other appropriate contact. • Conducted an online survey and analyzed data we obtained to evaluate the state agencies' satisfaction with CDT's services and to identify trends in the agencies' responses.
8	Determine statewide the number of legacy systems in need of modernization and determine those that are most critical. Furthermore, for the agencies with legacy systems needing modernization, determine whether they have documented modernization plans.	• Developed and included survey questions to assess state agencies' need to modernize their most important IT systems and whether they had documented modernization plans. • Analyzed the responses to determine the number of those IT systems requiring modernization.
9	Identify any recommendations that could improve or assist CDT's efforts to deliver digital services, develop innovative and responsive solutions for business needs, and provide assistance with IT projects and services.	• Worked with an IT consultant to identify best practices for delivering digital services and developing innovative solutions, such as establishing a repository of systems to enable reusability and minimize redundancy. Our work in other audit objectives also identified related recommendations. • Reviewed the roles and responsibilities of the Office of Data and Innovation related to delivering digital services.
10	Review and assess any other issues that are significant to the audit.	No other issues identified.

Source: Audit workpapers.

Assessment of Data Reliability

The U.S. Government Accountability Office, whose standards we are statutorily obligated to follow, requires us to assess the sufficiency and appropriateness of computer-processed information that we use to support our findings, conclusions, or recommendations. In performing this audit, we relied on electronic data files that we obtained from CDT related to staffing, IT project information, and IT procurement

information. To evaluate these data, we reviewed existing information about the data, interviewed staff knowledgeable about the data, and performed testing of the data. We found the staffing information to be reliable for our purposes. However, we found both the IT project information and the IT procurement information to be of undetermined reliability because the data were incomplete. Although we recognize that these limitations may affect the precision of the numbers we present, there is sufficient evidence in total to support our audit findings, conclusions, and recommendations.

STATE OF CALIFORNIA **GAVIN NEWSOM, Governor**

CALIFORNIA DEPARTMENT OF TECHNOLOGY
707 3rd Street,
West Sacramento, CA 95605
(916) 319-9223

Liana Bailey-Crimmins, Director
Jared Johnson, Chief Deputy Director

February 27, 2023

Grant Parks (*via GovOps Secretary Amy Tong)**
California State Auditor
621 Capitol Mall, Suite 1200
Sacramento, CA 95814

Dear Mr. Parks:

The California Department of Technology (CDT) appreciates the efforts of the California State Auditor's office in producing its most recent report. We agree that effective strategic planning, cybersecurity, and information technology (IT) project oversight are crucial to achieving successful outcomes for California and its residents. CDT exercises its authority in a collaborative, forward-thinking, and flexible manner that meets the business and operational needs of state entities responsible for operating the fourth-largest economy in the world. The data demonstrates that CDT performs effectively for the people of California, and for this reason, we disagree with the conclusions of the audit. ①

Of significant note, the Auditor did not include the impacts of the global pandemic over the last three years, and how CDT's leadership supported California's nation-leading response to COVID-19. This effort included 75 competitive procurements in a matter of weeks, seven statewide mission-critical systems implemented in a few months, a public website with over 20 data dashboards visited over 100 million times, and a statewide vaccine program enabled by technology. ②

The following response addresses each of the recommendations. ③

Recommendation 1: The Legislature should revise state law to clarify CDT's roles, responsibilities, and priorities for strategically guiding the State's acquisition, management, and use of IT.

CDT Response: CDT has ensured that the state's IT effectively and securely serves Californians. CDT welcomes further clarification of its roles and responsibilities. However, CDT considers its current Strategic Planning, IT modernization, and Technology reuse processes to be the most appropriate for the State.

CDT's Strategic Plan-Vision 2023 represents the statewide roadmap for IT investment and requires the collective efforts of all state entities to accomplish its goals. Agency ④

* California State Auditor's comments begin on page 69.

California State Auditor
February 27, 2023
Page 2

Information Officers (AIOs) and Departmental Chief Information Officers (CIOs) achieve the Strategic Plan objectives through multiple programs, processes, and outcomes as defined by Cal-Secure, the California State Broadband Action Plan, and the pending Digital Strategy. Alignment also occurs through the Budget Change
⑤ Proposal (BCP) and IT Project Approval Lifecycle (PAL) processes. As part of the implementation of Vision 2023, the Legislature provided funding for the Technology Modernization Fund (TMF), Technology Stabilization Fund (TSF), and Digital Innovation Fund (DIF). This enabled formation of departmental challenge teams to identify impactful IT modernization, stabilization, and process improvement initiatives, each with its objectives and metrics for measuring outcomes. CDT continues to report the
⑥ status of its strategic planning to the Legislature via the IT Annual Report, pursuant to Government Code (GC) section 11545.

⑦ CDT has identified 300 critical IT systems and is developing a plan to assess and prioritize high-risk, critical systems for modernization. CDT continues to report the status of its progress to the Legislature, pursuant to GC section 11546.45.

⑧ CDT has taken multiple steps to ensure efficient use and avoid duplication of IT capabilities and identifies IT solutions that may be repurposed for projects evaluated through the BCP and PAL processes. In addition, CDT has taken steps to consolidate shared services and contracts that achieve volume discounts for products and services like Storage as a Service and statewide productivity tools.

Recommendation 2: The Legislature should require CDT to create and lead an inter-organizational task force to assess IT staffing problems in the State and to issue recommendations to increase the State's hiring and retention rates of highly qualified IT personnel.

CDT Response: CDT acknowledges that IT workforce development is a significant challenge. CDT is collaborating with the Government Operations Agency and California Department of Human Resources through the "Work for California" Campaign, a targeted initiative to help address the statewide IT staffing issue.

Recommendation 3: The Legislature should require CDT to develop a plan for determining the overall statewide information security status of the State's reporting entities.

CDT Response: CDT'S statewide security strategy has improved the state's security posture and continues to expand its cybersecurity capabilities. CDT and California Cybersecurity Integration Center (Cal-CSIC) partners released Cal-Secure in 2021 – a nationally recognized gold standard in improving cyber security and privacy protections for state and local entities.

California State Auditor
February 27, 2023
Page 3

CDT has a comprehensive view of the cybersecurity status of 120 state entities based on various metrics and monitoring through the State Operations Center (SOC), including through Independent Security Assessment (ISA) scores and critical gap areas at multiple levels, as shown below: (9)

Security Metrics	2019	2022
ISA Score	53	55
Endpoint Hardening Score	54%	59%
Phishing Click Rates	22%	14%
Defended External Access	64	100
Passwords Compromised	11%	3%

In 2022, CDT expanded its no-cost SOC services to state and local entities needing more operational security controls. As of early 2023, CDT provides this expanded service to almost 40 entities, with an additional 15 in the queue for onboarding and implementation. CDT agrees with the Auditor that further marketing is needed.

Recommendation 4: The Legislature should make changes to ensure the independence of IT project oversight.

CDT Response: The placement of CDT as an oversight agency within the Executive Branch is the intentional result of the 2012 Governor's Reorganization Plan, approved by the Legislature. Consistent with the statute, CDT has adopted a federated model that establishes policy and provides oversight and guidance to state entities through AIOs and departmental CIOs. Rather than a "top-down" approach to oversight, GC section 11545 requires collaboration and consultation with state entities to ensure the efficacy of the processes and policies CDT is issuing. GC section 11546 grants CDT broad discretion to determine the most effective approach to project management. Accordingly, CDT has adopted an objective and helpful approach to IT planning, procurement, and project oversight that scales to meet individual department needs. The focus is on successful project outcomes through early engagement, which avoids punitive actions such as project suspension or termination. (10)

Recommendation: 5: CDT should develop a policy or procedure that documents the required elements of its strategic plan.

CDT Response: CDT believes our approach to strategic planning is the most effective for California. However, CDT will consider additional policies or procedures that clarify our strategic planning process. (4)

Recommendation 6: CDT should perform increased security outreach with reporting entities.

California State Auditor
February 27, 2023
Page 4

CDT Response: CDT and Cal-CSIC are the first lines of defense against threats to the state's IT infrastructure. CDT is aware of the constantly evolving threat landscape and
⑨ has a comprehensive picture of the cybersecurity status of 120 state entities. CDT continuously monitors threats through various cybersecurity metrics and the SOC, proving our approach is successful. CDT understands continuous improvement is necessary and will consider Auditor's recommendations.

Recommendation 7: Improve the effectiveness of the PAL Process

CDT Response: CDT's PAL process has achieved its intended purpose - providing a framework and guidance to plan and implement IT projects. Since its implementation
⑤ in 2016, CDT has helped 231 IT projects achieve PAL completion. CDT ensures alignment of projects with statewide strategic goals and has introduced agile and modular project methodologies where appropriate. As a result, California's IT project
⑪ metrics remain consistently higher than the industry average:

2018 - 2022	California State	Industry Average
Successful Projects	62.5%	31%
Challenged Projects	37.5%	50%
Failed Projects	0%	19%

*Industry average statistics obtained from the nationally recognized Standish Group.

CDT fully complies with its strategic planning, cybersecurity, and project oversight
⑫ responsibilities. While we disagree with many of the conclusions and implications of the audit findings, the State Auditor's recommendations will be considered. Please contact Kirk Marston, Internal Supervising Auditor, at kirk.marston@state.ca.gov if you have questions.

Sincerely,

Liana Bailey-Crimmins
Director
California Department of Technology

cc: Amy Tong, Secretary, Government Operations Agency
Miriam Ingenito, Undersecretary, Government Operations Agency
Jared Johnson, Chief Deputy Director, California Department of Technology

CALIFORNIA STATE AUDITOR'S COMMENTS ON THE RESPONSE FROM THE CALIFORNIA DEPARTMENT OF TECHNOLOGY

To provide clarity and perspective, we are commenting on the response to our audit from CDT. The numbers below correspond to the numbers we have placed in the margin of the response.

We stand by our conclusions. We have based our conclusions on sufficient and appropriate evidence, as auditing standards require. Throughout our report, we describe the evidence we reviewed and the shortcomings of CDT's processes. (1)

Our audit focused on CDT's oversight of state IT projects and the State's safeguards against cybersecurity threats, which included concerns we have reported for about 10 years. CDT's actions taken during the COVID-19 pandemic were not the focus of the audit and were taken under emergency, exceptional circumstances. However, we do acknowledge the Office of Data and Innovation's work in creating a COVID-19 informational website—covid.ca.gov—on page 7 of our report, and discuss the impact the pandemic has had on other IT projects, such as EDD's modernization project. (2)

CDT summarized our recommendations in its response. Our complete list of recommendations is presented starting on page 39. (3)

We believe CDT misunderstands its role in strategic planning. As we state on page 36, state law clearly directs CDT to take all appropriate and necessary steps to implement the annual IT strategic plan. CDT's challenges with strategic planning are consistent with a problem we identified about 10 years ago, and our review during this audit demonstrates that CDT's weaknesses in strategic planning remain, a concern that some of our survey respondents also expressed, as noted in the textbox on page 12. Further, nearly 40 percent of agencies responding to our survey do not believe CDT adequately fulfills its main role as shown on page 46, while many agencies have responded that they do not use CDT's oversight, consulting, and information security services, as shown on pages 50, 52, and 53, respectively. By not incorporating best practices into its IT strategic planning, such as establishing concrete performance metrics related to its broad goals, CDT lacks accountability measures to track the State's progress toward achieving the State's IT strategic goals and demonstrate that the State is meeting them. (4)

CDT's response does not address the concerns we identify in our report. CDT is mischaracterizing its own PAL process when it states that alignment with strategic goals occurs through the PAL process. As we state on page 25, Stage 1 of PAL requires an agency to describe how the proposed project will help achieve only the agency's strategic business plans, rather than statewide IT strategic goals. As a result, CDT forgoes an opportunity early in the process to verify that the proposed project aligns with statewide strategic goals. (5)

⑥ CDT's annual reports lack important context. As we note on page 11, its annual reports generally do not indicate the extent to which a strategic goal was met, include context by which to interpret the metrics, or indicate to which strategic goal the metric refers.

⑦ CDT's response is misleading. Although it asserts it has identified 300 critical systems, it does not make clear that it still must determine which of those systems require stabilization or modernization. Further, the list is not complete because it only includes systems from 60 state agencies. CDT has yet to establish and document a process to identify and assess IT systems that are outdated or difficult to support and require modernization, nor has it developed a timeline for doing so, as we state on page 14. We recommended on page 39 that the Legislature require CDT to develop a plan by July 1, 2023, for satisfying its statutory requirement to identify, assess, and prioritize modernizing high-risk, critical IT systems.

⑧ Although CDT asserts that it has taken multiple steps to avoid duplication of IT capabilities, it did not provide any details in its response, and this statement does not align with what we found during our audit. As we state on page 16 of our report, as of November 2022, CDT was in the process of reviewing 86 IT projects. CDT could use the information it receives about these projects to identify requests that involve redundant or duplicative IT systems. However, it does not track and publish complete information that would enable reusability and minimize redundancy across IT proposals and projects, and it does not proactively work with agencies to identify and pursue opportunities for sharing technology.

⑨ CDT's statement that it has a comprehensive view of the cybersecurity status is misleading. Although CDT has collected information about various aspects of some state agencies' information security development, it has yet to specifically determine the effectiveness of the cybersecurity programs that each of the State's 107 reporting entities have implemented, and thus, lacks a comprehensive understanding of the State's information security status. As we state on page 17, CDT currently relies on maturity metrics—which are fully based on independently validated information—to objectively summarize each reporting entity's information security status. However, CDT has achieved limited coverage. Specifically, as of December 2022, CDT calculated maturity metrics for only 43 of the State's 107 reporting entities, as page 19 states.

⑩ CDT misunderstands our concern and the importance of independent oversight. Specifically, as we state starting on page 31, CDT's role as advisor to the Governor and CDT's blurring of its planning and oversight roles creates a potential conflict with CDT's ability to carry out its oversight activities in an objective and independent manner. CDT's pattern of not taking adequate action when projects are struggling further illustrates our concerns about its independence. As we describe on page 27, despite its significant authority, CDT has not always adequately intervened to ensure that agencies resolve problems that its project oversight identifies in IT projects. We also state on page 30 that in eight of our reports over the past 10 years, we noted CDT's history of not sufficiently intervening to resolve ongoing problems in IT projects.

CDT did not provide the IT project metrics it cites in its response to us during the audit. Moreover, its response does not provide any context about the number, size, or complexity of the projects it analyzed. Nevertheless, we note on page 26 that CDT has been unable to provide a documented approach for measuring the effectiveness of PAL. Because many of the IT projects CDT approves under the PAL process cost millions of dollars, the State needs to be certain that the process is effective. As we recommend on page 41, CDT should develop internal metrics that include information on each project's size, the timeliness with which a solution was procured, the length of time to complete each stage of PAL, the degree to which an implementation was successful, and the degree to which the project was completed on time and within budget. (11)

CDT's response suggests that it believes it has successfully executed its planning, cybersecurity, and project oversight responsibilities. We disagree. We discuss CDT's deficiencies in these areas throughout the report, and we provide recommendations for how CDT could implement a robust strategic plan for IT statewide, clearly set priorities for addressing the State's IT needs, and demonstrate urgency in preparing for and responding to cybersecurity threats. (12)