Report 20-11
September 2020

IT Needs Assessment, Procurement, and Security

Department of Administration

STATE OF WISCONSIN



Legislative Audit Bureau

Report 20-11
September 2020

IT Needs Assessment, Procurement, and Security

Department of Administration

Joint Legislative Audit Committee Members

Senate Members:	Assembly Members:
Robert Cowles, Co-chairperson	Samantha Kerkman, Co-chairperson
Chris Kapenga	John Macco
Alberta Darling	John Nygren
Janet Bewley	Melissa Sargent
Tim Carpenter	Katrina Shankland

Report 20-11
September 2020

State Auditor
Joe Chrisman

Deputy State Auditor For Performance Evaluation
Dean Swenson

Financial Audit Director
Kendra Eppler

Team Leaders
Derek Hippler
Noah Natzke

Evaluators
Stephanie Besst
Nehemiah Chinavare
James Malone
Sam Rebenstorf
Ross Ryan
Kendall Vega

Auditors
Bruce Flinn
Jennifer Multerer
Colin Shogren
Elizabeth Wilson

Publications Designer and Editor
Susan Skowronski

LEGISLATIVE AUDIT BUREAU

The Legislative Audit Bureau supports the Legislature in its oversight of Wisconsin government and its promotion of efficient and effective state operations by providing nonpartisan, independent, accurate, and timely audits and evaluations of public finances and the management of public programs. Bureau reports typically contain reviews of financial transactions, analyses of agency performance or public policy issues, conclusions regarding the causes of problems found, and recommendations for improvement.

Reports are submitted to the Joint Legislative Audit Committee and made available to other committees of the Legislature and to the public. The Audit Committee may arrange public hearings on the issues identified in a report and may introduce legislation in response to the audit recommendations. However, the findings, conclusions, and recommendations in the report are those of the Legislative Audit Bureau.

The Bureau accepts confidential tips about fraud, waste, and mismanagement in any Wisconsin state agency or program through its hotline at 1-877-FRAUD-17.

For more information, visit *www.legis.wisconsin.gov/lab.*

Contact the Bureau at 22 East Mifflin Street, Suite 500, Madison, Wisconsin 53703; *AskLAB@legis.wisconsin.gov;* or (608) 266-2818.

CONTENTS

STATE OF WISCONSIN | Legislative Audit Bureau

22 East Mifflin St., Suite 500 ▪ Madison, WI 53703 ▪ (608) 266-2818 ▪ Hotline: 1-877-FRAUD-17 ▪ www.legis.wisconsin.gov/lab

Joe Chrisman
State Auditor

September 18, 2020

Senator Robert Cowles and
Representative Samantha Kerkman, Co-chairpersons
Joint Legislative Audit Committee
State Capitol
Madison, Wisconsin 53702

Dear Senator Cowles and Representative Kerkman:

As requested by the Joint Legislative Audit Committee, we have completed an evaluation of the State's information technology (IT) needs assessment and procurement processes, including for IT projects involving cloud computing services provided by firms. We also reviewed IT security at five state agencies.

The Department of Administration (DOA) is statutorily responsible for ensuring that executive branch agencies, other than the University of Wisconsin System, make effective and efficient use of IT resources. DOA must establish IT policies and procedures, which statutes require agencies to follow. Statutes also require DOA to monitor adherence to these policies and procedures.

We found that DOA and other state agencies did not consistently comply with various statutes and policies pertaining to IT projects, including large, high-risk IT projects. In addition, we found that DOA and other agencies did not consistently follow best practices for data security when completing projects involving cloud computing services provided by firms. We also identified concerns with IT security at five state agencies and have conveyed our specific concerns to DOA, which should take action to address them.

DOA needs to improve its oversight of IT projects, including by complying with statutory requirements. In addition, it should help state agencies to develop appropriate policies for contracting with firms that provide cloud computing services. We make a number of recommendations for improvements.

We appreciate the courtesy and cooperation extended to us by DOA. A response from DOA's secretary follows the Appendix.

Respectfully submitted,

Joe Chrisman
State Auditor

JC/DS/ss

Report Highlights ■

The Board of Regents is statutorily responsible for overseeing IT projects in UW System.

The Board of Regents of the University of Wisconsin (UW) System is statutorily responsible for overseeing information technology (IT) projects in UW System. Statutes permit UW institutions to implement only those IT projects that have been approved by the Board of Regents.

DOA is statutorily responsible for ensuring that executive branch agencies make effective and efficient use of IT resources.

The Department of Administration (DOA) is statutorily responsible for ensuring that executive branch agencies, other than UW System, make effective and efficient use of IT resources. DOA must establish IT policies and procedures, which statutes require agencies to follow. Statutes require DOA to monitor adherence to these policies and procedures.

To complete our audits, we:

- evaluated how 5 UW institutions and 6 state agencies managed their IT needs assessment and procurement processes for IT projects, including projects involving cloud computing services provided by firms;

- surveyed 45 state agencies and 13 UW institutions about IT needs assessment and procurement, cloud computing, and IT security issues; and

- assessed IT security at a different set of 5 UW institutions and 5 state agencies.

A comprehensive evaluation of the costs of IT projects or the management of individual IT projects by UW institutions and state agencies was not in the scope of this evaluation.

Report 20-10 presents the results of our analyses for UW System, and report 20-11 presents the results of our analyses for DOA. Report 20-12 presents the results of our analysis of the master lease program, which DOA administers to provide state agencies, including itself, with funding for IT systems and other projects.

UW System

Statutes require the Board of Regents to promulgate policies for monitoring large, high-risk IT projects.

Statutes require the Board of Regents to promulgate policies for monitoring large, high-risk IT projects. These policies indicate that such projects include those that cost or are expected to cost more than $1.0 million. They also indicate that all such projects are managed and monitored by UW System Administration.

We analyzed how five UW institutions assessed their IT needs and procured goods and services for 10 projects, as well as how they managed data security and other issues for 7 projects that involved cloud computing services provided by firms. These 17 projects included 13 large, high-risk IT projects and were managed by UW System Administration, UW-Eau Claire, UW-Madison, UW-Milwaukee, and UW-Stevens Point.

We found that UW institutions did not consistently comply with various statutes, policies, and best practices, as shown in Table 1.

UW System Administration should address the IT security concerns that we found.

We found IT security concerns in our prior audits of UW System. In our current audit, we reviewed IT security at five UW institutions and found a number of concerns. UW System Administration should address each of the IT security concerns that we found, and it should ensure that all UW institutions, including itself, comply with its policies and procedures.

The Board of Regents needs to improve its oversight of IT projects, including large, high-risk IT projects.

The Board of Regents needs to improve its oversight of IT projects, including large, high-risk IT projects. UW System Administration should work with the Board of Regents to require the Board of Regents to approve all IT contracts that are more than $1.0 million. In addition, UW System Administration should work with the Board of Regents to establish an IT projects committee of the Board of Regents to help oversee IT projects.

Table 1

Key Audit Findings for UW System
Report 20-10

Needs Assessment and Planning UW System Administration did not include all statutorily required information in the IT strategic plan it provided to the Board of Regents for March 2020 *(p. 18)*.
UW institutions did not consistently comply with Board of Regents policies because they did not include all required information in the planning documents for large, high-risk IT projects *(p. 19)*.
Project Approval UW System Administration and UW-Madison implemented IT projects before obtaining the statutorily required approval from the Board of Regents to do so *(p. 20)*.
Procurement UW System Administration did not comply with Board of Regents policies because it did not require UW institutions to submit to it certain information about large, high-risk IT projects *(p. 22)*.
UW-Madison did not review the terms of a consortium's contract through which it purchased services in November 2017 *(p. 23)*.
UW System Administration did not comply with statutes that require it to report each quarter to the Board of Regents on the expenditures of projects with open-ended contracts *(p. 24)*.
UW institutions did not comply with statutes that require them to include in contracts for large, high-risk IT projects a stipulation that the Board of Regents must approve any order or amendment that would change the contract scope and increase the contract price *(p. 25)*.
UW-Madison did not have a contract with a firm over at least a six-month period in 2018 when a project was ongoing. UW-Stevens Point did not contractually require a firm to pay monetary penalties for not completing work on time for a large, high-risk IT project *(p. 26)*.
Project Reporting UW System Administration did not include information about all large, high-risk IT projects in the semiannual reports submitted to the Joint Committee on Information Policy and Technology from March 2014 through March 2020, or accurate and complete information about the projects that were included *(p. 28)*.
Cloud Computing UW institutions did not consistently evaluate in writing the advantages and disadvantages of transitioning to cloud computing services provided by firms *(p. 36)*.
UW institutions did not consistently follow best practices for data security when completing projects involving cloud computing services provided by firms *(p. 37)*.
IT Security UW System Administration did not develop comprehensive IT security policies and procedures, and we found 46 concerns pertaining to IT security at the five UW institutions we reviewed *(pp. 44-45)*.
Board of Regents Oversight Board of Regents policies do not require UW institutions to obtain Board of Regents approval to execute all IT contracts of more than $1.0 million *(p. 48)*.

DOA

Statutes require DOA to adopt policies pertaining to large, high-risk IT projects.

Statutes require DOA to adopt policies pertaining to large, high-risk IT projects. Such projects either exceed $1.0 million or are vital to the functions to executive branch agencies, other than UW System. Statutes indicate that DOA must require each executive branch agency other than UW System to annually submit to it a strategic plan for using IT to carry out the agency's functions in the following fiscal year.

We analyzed how six state agencies assessed their IT needs and procured goods and services for 12 projects, as well as how they managed data security and other issues for 6 projects that involved cloud computing services provided by firms. These 18 projects included 12 large, high-risk IT projects and were managed by one or more of six agencies: DOA; the departments of Children and Families (DCF), Employee Trust Funds (ETF), Health Services (DHS), and Transportation (DOT); and the State of Wisconsin Investment Board (SWIB).

We found that state agencies did not consistently comply with various statutes, policies, and best practices, as shown in Table 2.

DOA should work with state agencies to address the IT security concerns that we found.

We found IT security concerns in prior audits of DOA. In our current audit, we reviewed IT security at five state agencies and found a number of concerns. DOA should work with agencies to address the IT security concerns that we found, and it should ensure that all agencies, including itself, comply with its policies.

DOA needs to improve its oversight of IT projects and IT security.

DOA needs to improve its oversight of IT projects, including large, high-risk IT projects. DOA should consistently comply with statutory requirements pertaining to its oversight of IT projects, including large, high-risk IT projects. DOA should also help state agencies to develop appropriate policies for contracting with firms that provide cloud computing services. If the Joint Committee on Information Policy and Technology met more regularly, it could monitor the status of large, high-risk IT projects.

Table 2

Key Audit Findings for DOA
Report 20-11

Needs Assessment and Planning DOA did not require state agencies to include all statutorily required information in their March 2019 IT strategic plans *(p. 18)*.
DOA did not comply with statutes because it did not submit statewide IT strategic plans to the Joint Committee on Information Policy and Technology in recent years (*p. 19*).
DOA did not comply with its policies because it did not ensure that an interagency committee conducted technical reviews of all large, high-risk IT projects *(p. 20)*.
Procurement DOA did not comply with statutes because it did not review and approve eight contracts, which totaled an estimated $93.5 million and were executed from August 2013 through August 2018, for five large, high-risk IT projects *(p. 20)*.
None of the seven contracts we reviewed, which were executed from August 2013 through August 2018, contained the statutorily required stipulation that DOA must approve certain orders and amendments *(p. 21)*.
Project Reporting State agencies did not consistently provide DOA with accurate and complete information about their large, high-risk IT projects from September 2014 through September 2019 *(p. 22)*.
DOA did not submit the statutorily required semiannual reports to the Joint Committee on Information Policy and Technology from March 2014 through September 2019 *(p. 24)*.
Cloud Computing DOA established few policies that specifically address how state agencies are to acquire cloud computing services from firms *(p. 25)*.
Only 13 state agencies indicated that they had policies and procedures governing the procurement and management of cloud computing services provided by firms *(p. 26)*.
State agencies did not consistently evaluate in writing the advantages and disadvantages of transitioning to cloud computing services provided by firms *(p. 29)*.
Agencies did not consistently follow best practices for data security when completing projects involving cloud computing services provided by firms *(p. 30)*.
IT Security Policies, standards, and procedures at the five state agencies we reviewed did not include all anticipated elements relevant to IT security, and we found 23 concerns pertaining to IT security *(p. 37)*.

Master Lease Program at DOA

Statutes authorize DOA to administer the master lease program, through which state agencies may fund their purchases of IT systems and certain other assets. Statutes also allow UW System, the Legislature, and the courts to use the program to fund purchases.

State agencies apply for master lease funding from DOA, which decides whether to approve their applications. The Legislature is not involved in approving the applications.

To obtain master lease funding, DOA borrows funds from a bank and periodically issues certificates of participation.

To obtain master lease funding, DOA borrows funds from a bank and periodically issues certificates of participation, which are a type of debt instrument similar to bonds. The certificates are not a general obligation debt of the State and are not backed by the full faith and credit of the State. Agencies repay master lease funding, plus interest and administrative fees, from the amounts appropriated to them.

We found concerns with DOA's program policies, consideration of applications for master lease funding, oversight of the program, and statutorily required reporting, as shown in Table 3.

Table 3

Key Audit Findings for the Master Lease Program at DOA
Report 20-12

From FY 2014-15 through the first half of FY 2019-20, $142.1 million of the $157.9 million (90.0 percent) of master lease funding approved by DOA was for 28 IT projects *(p. 13)*.
Projects managed by DOA accounted for $118.3 million of the $142.1 million (83.3 percent) in total master lease funding for IT projects *(p. 14)*.
From FY 2014-15 through the first half of FY 2019-20, state agencies made a total of $154.4 million in master lease payments, including repayment of principal, interest, and administrative fees *(p. 16)*.
As of December 15, 2019, the principal balance of all outstanding certificates of participation totaled $88.6 million *(p. 16)*.
DOA's program policies were incomplete and outdated *(p. 17)*.
DOA did not document the reasons for approving any of the 28 applications for master lease funding for IT projects *(p. 19)*.
DOA permitted state agencies, including itself, to obtain a total of $4.4 million more in master lease funding than the amounts it had approved for eight projects from FY 2014-15 through the first half of FY 2019-20 *(p. 20)*.
From October 2014 through October 2019, DOA did not submit statutorily required annual reports on master lease funding for IT projects *(p. 22)*.

Recommendations

In report 20-10, we include recommendations for UW System Administration to report to the Joint Legislative Audit Committee by January 15, 2021, on efforts to:

- ☑ improve the IT needs assessment and planning processes (*pp. 18* and *19*);
- ☑ improve the IT project approval process (*p. 21*);
- ☑ improve IT procurement (*pp. 22*, *23*, *24*, *25*, *26*, *26*, and *27*);
- ☑ improve project reporting (*p. 29*);
- ☑ improve cloud computing policies (*pp. 32* and *33*);
- ☑ improve cloud computing needs assessment and procurement (*p. 36*);
- ☑ improve data security for cloud computing projects (*p. 39*); and
- ☑ work with the Board of Regents to modify policies (*p. 49*) and create an IT Projects Committee of the Board of Regents (*p. 51*).

In report 20-11, we include recommendations for DOA to report to the Joint Legislative Audit Committee by January 15, 2021, on efforts to:

- ☑ improve the IT needs assessment and planning processes (*pp. 19, 19,* and *20*);
- ☑ improve IT procurement (*pp. 21* and *22*);
- ☑ improve project reporting (*pp. 24* and *24*);
- ☑ improve cloud computing policies (*p. 26*);
- ☑ improve data security for cloud computing projects (*p. 33*); and
- ☑ improve its oversight (*pp. 41* and *42*).

In report 20-10 and report 20-11, we include recommendations for UW System Administration (*p. 45*) and DOA (*p. 37*) to report to the Joint Legislative Audit Committee by November 13, 2020, on their efforts to improve IT security.

In report 20-12, we include recommendations for DOA to report to the Joint Legislative Audit Committee by January 15, 2021, on efforts to:

- ☑ revise its master lease policies (*p. 18*);
- ☑ document its reviews of applications for master lease funding (*p. 20*);
- ☑ ensure state agencies do not obtain more master lease funding than the approved amounts (*p. 21*);
- ☑ establish the maximum length of time that state agencies have to obtain master lease funding (*p. 22*); and
- ☑ annually submit statutorily required reports to the Joint Committee on Information Policy and Technology (*p. 23*).

Issues for Legislative Consideration

In report 20-11, we note that the Legislature could consider modifying statutes to:

- allow governmental bodies to convene in closed session in order to discuss IT security issues *(p. 38);*
- focus DOA's IT oversight duties (*p. 42*); and
- increase the dollar threshold of a large, high-risk IT project (*p. 42*).

In report 20-12, we note that the Legislature could consider modifying statutes to require DOA to:

- obtain its approval before approving certain applications for master lease funding (*p. 23*); and
- report to the Joint Legislative Audit Committee annually on the use of master lease funding (*p. 23*).

■ ■ ■ ■

Introduction ■

DOA is statutorily responsible for ensuring that executive branch agencies, other than UW System, make effective and efficient use of the State's IT resources.

Under s. 16.971 (2), Wis. Stats., DOA is responsible for ensuring that executive branch agencies, other than UW System, make effective and efficient use of the State's IT resources. To that end, statutes require DOA, in cooperation with state agencies, to establish policies, procedures, and planning processes for administering IT services. Statutes require agencies to follow these policies, procedures, and processes and DOA to monitor adherence to them.

Statutes require DOA to perform certain IT duties for other state agencies, including:

- developing and maintaining IT resource planning and budgeting, as well as procedures to ensure IT resource planning and sharing between agencies;

- implementing, operating, maintaining, and upgrading an enterprise resource planning system capable of providing IT services to all agencies in specified areas, including payroll and financial services, procurement, and human resources;

- developing review and approval procedures that encourage the timely and cost-effective acquisition of hardware, software, and professional services, and reviewing and approving the acquisition of such items and services under these procedures;

- gathering, interpreting, and disseminating information on new technological developments, management techniques, and IT resource capabilities;

- ensuring all agencies operate with clear guidelines and standards in IT systems development, and that they employ good management practices; and

- ensuring all state data processing facilities develop proper privacy and security procedures and safeguards.

Statutes require DOA to adopt policies pertaining to IT projects that either exceed $1.0 million or are vital to the functions of an executive branch agency other than UW System. Such projects are commonly known as large, high-risk IT projects. Statutes require DOA to promulgate a definition of and methodology for identifying such projects, policies and procedures for routinely monitoring such projects, and requirements for reporting changes to DOA in project cost estimates or completion dates.

DOA must require each executive branch agency other than UW System to annually submit to it a strategic plan for using IT to carry out the agency's functions in the following fiscal year.

Statutes indicate that DOA must require each executive branch agency other than UW System to annually submit to it a strategic plan for using IT to carry out the agency's functions in the following fiscal year. In these plans, agencies must identify all proposed projects that serve their business needs as well as the justification and priority for undertaking each project. Statutes indicate that agencies are allowed to implement only those projects that have been approved by DOA.

Questions have been raised about how state agencies assess the need for IT projects, procure goods and services for projects, manage and oversee projects that involve cloud computing services provided by firms, and ensure IT security. This evaluation considers these issues in agencies other than UW System. In report 20-10, we considered these issues in UW System, which is statutorily responsible for managing its IT projects separate from other agencies. In report 20-12, we considered DOA's management of the master lease program that agencies can use to fund IT and other types of projects.

We previously conducted evaluations that analyzed the State's use of IT, including *Information Technology Projects* (report 07-5), *Consolidation of Administrative Functions and the ACE Initiative* (report 09-9), and *Oversight of the Human Resource System and Payroll and Benefits Processing* (report 14-4) at UW System. We analyzed IT security issues in our audits of the financial statements for the State of Wisconsin for fiscal year (FY) 2014-15 (report 16-2), FY 2015-16

(report 17-4), FY 2016-17 (report 18-3), FY 2017-18 (report 18-20), and FY 2018-19 (report 19-30). We reported a variety of IT security concerns in these reports, including concerns with the lack of executive branch IT policies and standards and DOA's oversight of the State's IT environment.

To complete this evaluation, we analyzed how six state agencies—DOA, DCF, ETF, DHS, DOT, and SWIB—assessed their IT needs and procured goods and services for 12 projects, as well as how they managed data security and other issues for 6 projects that involved cloud computing services. We selected these projects based on multiple risk factors, including project costs and whether a given project involved sensitive data. The cloud computing projects involved cloud computing services provided by firms, rather than the cloud computing services that DOA provided agencies through its data center. Finally, we reviewed IT security at a different set of five state agencies. A comprehensive evaluation of the costs of IT projects or the management of individual IT projects by agencies was not in the scope of this evaluation.

In January 2020, we surveyed 45 state agencies about IT needs assessment and procurement, cloud computing, and IT security issues.

In January 2020, we surveyed 45 state agencies about IT needs assessment and procurement, cloud computing, and IT security issues. Every agency responded to our survey. A total of 31 agencies indicated that they used cloud computing services provided by firms. Survey respondents indicated that they most commonly used such services for email, office productivity such as word processing, and document management. The Appendix summarizes the survey responses.

■ ■ ■ ■

IT Needs Assessment and Procurement ■

We evaluated DOA's oversight of how state agencies assessed their IT needs and procured goods and services for projects.

We evaluated DOA's oversight of how state agencies assessed their IT needs and procured goods and services for projects. To do so, we reviewed 12 projects managed by one or more of the following six agencies: DOA, DCF, DHS, ETF, DOT, and SWIB. We found that DOA did not require agencies to include all statutorily required information in their March 2019 IT strategic plans or comply with its own policies because it did not ensure that an interagency committee conducted technical reviews of large, high-risk IT projects. In addition, DOA did not submit statutorily required semiannual reports to the Joint Committee on Information Policy and Technology from March 2014 through September 2019. We make a number of recommendations to DOA for improvements.

Projects

The 12 projects we reviewed began from FY 2012-13 through FY 2018-19 and included:

- DOA's State Transforming Agency Resources (STAR), which implemented an enterprise resource planning system that includes accounting, payroll, and purchasing functions;
- DCF's Child Support Document Generation Subsystem Replacement, which replaced the system that local child support agencies use to generate documents for child support cases;

- DHS's Electronic Insurance-Based Billing System, which created a system that electronically bills insurers for claims initially paid by Medical Assistance, but for which private insurance is responsible;

- DOA's Genesys, which was intended to replace the automated call distribution system that state agencies used to route incoming calls but was cancelled before project completion;

- SWIB's Financial and Administrative Solution, which integrated SWIB's accounting and human resources functions with its investment management system and aligned those systems with STAR;

- DOT's DT 4000 Crash Database, which replaced an existing system for collecting and managing motor vehicle crash data;

- ETF's Automated Call Distribution System, which replaced an automated telephone call distribution system provided by DOA;

- DOA's Splunk, which implemented a system that allows DOA to audit, monitor, and prevent unauthorized access to state IT systems;

- DHS's Medicaid Management Information System Enhancement, which is expected to upgrade data analysis, enrollment services, and care management functions;

- DCF's Benefit Recovery and Investigation Tracking System, which is expected to create a system for DCF and DHS to track public assistance fraud and claims investigations;

- SWIB's eFront, which is expected to create a system to automate trading activities and provide analytical tools for monitoring investment portfolios; and

- DOT's Advanced Traffic Management System, which is expected to create a system to monitor, manage, and alert the public about highway traffic conditions.

Nine of the 12 projects we reviewed were reported as large, high-risk IT projects.

As shown in Table 4, 8 of the 12 projects we reviewed were completed, and 4 projects were ongoing at the time of our fieldwork. State agencies reported 9 of the 12 projects as large, high-risk IT projects, but they did not report Genesys, Automated Call Distribution System, and Splunk as large, high-risk IT projects.

Table 4

State Agency IT Projects Reviewed

	State Agency	Information Provided by State Agencies		
		Start Date	Completion Date	Expenditures
Completed Projects			**Actual**	
STAR	DOA	Jan. 2014	July 2016	$182,100,000[1]
Child Support Document Generation Subsystem Replacement	DCF	Sept. 2013	May 2019	21,900,000
Electronic Insurance-Based Billing System	DHS	Aug. 2015	Jan. 2020	14,600,000
Genesys[2]	DOA	April 2016	Mar. 2019	12,000,000
Financial and Administrative Solution	SWIB	Sept. 2014	Nov. 2016	4,800,000
DT 4000 Crash Database	DOT	Jan. 2015	Feb. 2017	2,300,000
Automated Call Distribution System[2]	ETF	May 2019	Aug. 2019	500,000
Splunk[2]	DOA	Feb. 2019	Mar. 2020	78,600[3]
Ongoing Projects			**Estimated**	
Medicaid Management Information System Enhancement	DHS	Aug. 2018	Sept. 2021	72,300,000
Benefit Recovery and Investigation Tracking System	DCF	Jan. 2013	Dec. 2022	6,600,000
eFront	SWIB	Sept. 2016	July 2020	3,800,000
Advanced Traffic Management System	DOT	Aug. 2014	July 2020	3,500,000

[1] Project expenditures through June 2019, including $50.3 million in maintenance and operations expenditures, as reported by DOA to the Joint Legislative Audit Committee.

[2] These projects were not reported as large, high-risk IT projects.

[3] Excludes DOA staff costs, which DOA did not provide to us.

Needs Assessment and Planning

As noted, statutes indicate that DOA must require each executive branch agency other than UW System to annually submit to it an IT strategic plan to carry out the agency's functions in the following fiscal year. In these plans, agencies must include information about all proposed projects that address their business needs, the justification for and anticipated benefits of each project, the priority for undertaking each project, and whether each project could be completed from available resources or would require additional resources. Completing these plans helps DOA and agencies appropriately assess the need for projects and plan for them.

Statutes require state agencies to provide their IT strategic plans to DOA by each March 1, and they permit agencies to implement only those projects approved by DOA. DOA indicated that it had not rejected a strategic plan in the past five years.

State agencies did not consistently include all projects and all statutorily required information in the IT strategic plans they submitted to DOA in recent years.

We found that state agencies did not consistently include all projects and all statutorily required information in the IT strategic plans they provided to DOA in recent years. For example:

- DCF excluded some project costs, including for software licensing and a consultant, for the Child Support Document Generation Subsystem Replacement in its four strategic plans from March 2015 through March 2018;

- DHS excluded its own project-related staff costs for the Electronic Insurance-Based Billing System in its three strategic plans from March 2016 through March 2018; and

- SWIB did not include eFront in its March 2017 and March 2018 strategic plans.

DOA did not require state agencies to include all statutorily required information in their March 2019 IT strategic plans.

DOA provided state agencies with written instructions on the types of information to include in their IT strategic plans. We found that DOA's instructions for the March 2019 plans did not require agencies to include all statutorily required information, including the need, anticipated benefit, and priority for each project. These instructions also advised agencies to include only those projects that were expected to involve DOA staff. We reviewed the March 2019 plans submitted by DCF, ETF, DHS, DOT, and SWIB and found that these agencies followed DOA's guidance for the projects we reviewed. After we asked DOA why it did not require agencies to include all statutorily required information in their March 2019 plans, DOA provided new instructions that required agencies to do so in their March 2020 plans.

DOA should consistently require state agencies to include all statutorily required information about all of their projects in their annual IT strategic plans. This information will allow DOA to assess the need, anticipated benefits, and priority for each project, make informed decisions about whether to approve or reprioritize projects, and help DOA to effectively oversee how agencies implement projects.

☑ Recommendation

We recommend the Department of Administration:

- *consistently require state agencies to include all statutorily required information about all of their projects in their annual information technology strategic plans; and*

- *report to the Joint Legislative Audit Committee by January 15, 2021, on its efforts to implement this recommendation.*

DOA did not comply with statutes because it did not submit statewide IT strategic plans to the Joint Committee on Information Policy and Technology in recent years.

Statutes require DOA to use the IT strategic plans provided by state agencies to formulate and biennially revise a statewide IT strategic plan, which DOA must submit no later than September 15 of each even-numbered year to the Joint Committee on Information Policy and Technology. We found that DOA created these statewide plans but did not submit them in 2014, 2016, or 2018. Instead, DOA posted these statewide plans to its website. DOA indicated that it intends to submit the 2020 statewide plan.

DOA should comply with statutes by submitting the statewide IT strategic plan to the Joint Committee on Information Policy and Technology every two years. Doing so will provide the Legislature with information needed to oversee projects undertaken by state agencies.

☑ Recommendation

We recommend the Department of Administration:

- *comply with statutes by submitting the statewide information technology strategic plan to the Joint Committee on Information Policy and Technology every two years; and*

- *report to the Joint Legislative Audit Committee by January 15, 2021, on its efforts to implement this recommendation.*

In 2011, DOA established policies that require a DOA-led interagency committee to conduct technical reviews of all large, high-risk IT projects. These reviews are intended to help guide project development, and they may also help identify the particular needs that projects should address. The available information indicates that the DOA-led interagency committee did not conduct these technical reviews for any of the 12 projects we reviewed.

DOA should comply with its policies by ensuring that the interagency committee conducts technical reviews of all large, high-risk IT projects. Doing so will help to ensure that state agencies effectively plan projects.

☑ Recommendation

We recommend the Department of Administration:

- *comply with its policies by ensuring that the interagency committee conducts technical reviews of all large, high-risk information technology projects; and*

- *report to the Joint Legislative Audit Committee by January 15, 2021, on its efforts to implement this recommendation.*

Procurement

DOA is statutorily prohibited from delegating to other state agencies, other than UW System, the authority to execute IT contracts without its review and approval of these contracts. DOA developed policies that indicate it must help to develop contracts for large, high-risk IT projects, but these policies do not require it to review and approve contracts for other projects.

DOA did not comply with statutes because it did not review and approve eight contracts, totaling an estimated $93.5 million, for five large, high-risk IT projects.

We found that DOA did not comply with statutes because it did not review and approve eight contracts, totaling an estimated $93.5 million and executed from August 2013 through August 2018, for five large, high-risk IT projects managed by DCF, DHS, and DOT. DOA indicated that it did not review any IT contracts developed by other state agencies because it believes such reviews are not feasible, agencies can develop the contracts without its assistance, and it reviews and approves summary project documentation, including a description and the estimated cost, before agencies execute contracts for projects expected to cost more than $50,000.

DOA should comply with statutes by reviewing and approving all IT contracts for other state agencies. Doing so will help DOA to fulfill its statutorily required oversight responsibilities and ensure that such contracts include sufficient legal and financial protections.

☑ Recommendation

We recommend the Department of Administration:

- *comply with statutes by consistently reviewing and approving all information technology contracts for other state agencies; and*

- *report to the Joint Legislative Audit Committee by January 15, 2021, on its efforts to implement this recommendation.*

Statutes require all contracts for large, high-risk IT projects to include a stipulation that DOA must approve any order or amendment that would change the contract scope and increase the contract price. Statutes allow state agencies to exclude such a stipulation if it would negatively affect contract negotiations or the number of potential bidders, a contract includes alternate provisions to ensure it is completed on time and on budget, and DOA submits alternative contract provisions to the Joint Committee on Information Policy and Technology for approval.

None of the seven contracts we reviewed contained the statutorily required stipulation that DOA must approve certain orders and amendments.

None of the seven contracts we reviewed, totaling an estimated $93.4 million and executed from August 2013 through August 2018, for five large, high-risk IT projects contained the statutorily required stipulation that DOA must approve an order or amendment that would change the contract scope and increase the contract price. DOA did not submit any of these contracts to the Joint Committee on Information Policy and Technology for approval, in part, because DOA did not review these contracts.

DOA should ensure that state agencies comply with statutes by including in contracts for large, high-risk IT projects a stipulation that it must approve any order or amendment that would change the contract scope and increase the contract price. It can do so by reviewing and approving these contracts, as is statutorily required. Doing so will help DOA to fully exercise its statutorily required oversight role.

☑ **Recommendation**

We recommend the Department of Administration:

- *ensure that state agencies comply with statutes by including in contracts for large, high-risk information technology projects a stipulation that it must approve any order or amendment that would change the contract scope and increase the contract price; and*

- *report to the Joint Legislative Audit Committee by January 15, 2021, on its efforts to implement this recommendation.*

Project Reporting

By each March 1 and September 1, statutes require DOA to submit to the Joint Committee on Information Policy and Technology a semiannual report on all large, high-risk IT projects in state agencies. Statutes require these reports to contain certain information, including:

- the status of each project, including any portion that has been completed;

- all project funding sources;

- original and updated cost projections and completion dates; and

- an explanation for any variation between the original and the updated costs and completion dates.

State agencies did not consistently provide DOA with accurate and complete information about their large, high-risk IT projects from September 2014 through September 2019.

To obtain the information needed to develop these semiannual reports, DOA requires state agencies to periodically provide information to it about all ongoing large, high-risk IT projects. We found that agencies did not consistently provide DOA with accurate and complete information about their large, high-risk IT projects from September 2014 through September 2019. DOA did not require agencies to provide information about the initial cost estimates or expected completion dates of their projects. We also found concerns with the final project cost information that agencies provided to DOA. For example:

- In July 2019, DCF reported a $21.9 million final cost for the Child Support Document Generation Subsystem Replacement, but this amount excluded $11.0 million in software licenses and network hosting infrastructure costs, which DCF indicated it had excluded because these costs were partially attributable to another project.

- In February 2017, DOT reported that it had completed the $2.3 million DT 4000 Crash Database on budget, but this amount excluded the costs of a data warehouse, which DOT had initially indicated would cost approximately $330,000.

Although DOA indicated that it attempted to identify the large, high-risk IT projects for which state agencies should have provided information, we found that agencies did not consistently include information about the 10 projects we reviewed. For example:

- DHS did not provide information to DOA about its Electronic Insurance-Based Billing System from August 2015 through July 2017;

- DHS did not provide information to DOA about its Medicaid Management Information System Enhancement from the project's beginning in August 2018 through January 2020;

- SWIB did not provide information to DOA about its Financial and Administrative Solution from January 2016 through November 2016;

- SWIB did not provide information to DOA about eFront from the project's beginning in September 2016 through January 2020; and

- DOT did not provide information to DOA about its Advanced Traffic Management System from November 2016 through December 2018.

DOA should ensure that state agencies consistently provide it with complete and accurate information about all ongoing large, high-risk IT projects. Doing so will help to ensure DOA is aware of large, high-risk IT projects and has accurate information in order to effectively oversee such projects.

☑ Recommendation

We recommend the Department of Administration:

- *ensure that state agencies consistently provide it with complete and accurate information about ongoing large, high-risk information technology projects; and*

- *report to the Joint Legislative Audit Committee by January 15, 2021, on its efforts to implement this recommendation.*

DOA did not submit the statutorily required semiannual reports to the Joint Committee on Information Policy and Technology from March 2014 through September 2019.

We found that DOA did not submit the statutorily required semiannual reports to the Joint Committee on Information Policy and Technology from March 2014 through September 2019. After we asked DOA about these reports in December 2019, DOA submitted the March 2020 report, which included 29 projects for which anticipated costs were listed. Nineteen projects were each anticipated to cost less than $5.0 million, six projects were each anticipated to cost between $5.0 million and $10.0 million, and four projects were each anticipated to cost more than $10.0 million. However, this report excluded information about the initial project cost estimates and completion dates for three of the four ongoing large, high-risk IT projects that we reviewed.

DOA should comply with statutes by consistently submitting semiannual reports about large, high-risk IT projects to the Joint Committee on Information Policy and Technology. In addition, it should ensure that these reports contain all statutorily required information about each project. Doing so will provide the Committee with information needed to oversee the State's IT efforts.

☑ Recommendation

We recommend the Department of Administration:

- *comply with statutes by consistently submitting semiannual reports about large, high-risk information technology projects to the Joint Committee on Information Policy and Technology;*

- *ensure that the submitted semiannual reports contain all statutorily required information about each project; and*

- *report to the Joint Legislative Audit Committee by January 15, 2021, on its efforts to implement these recommendations.*

■ ■ ■ ■

Cloud Computing ■

We evaluated how state agencies managed IT projects involving cloud computing services provided by firms.

We evaluated how state agencies managed IT projects involving cloud computing services provided by firms. To do so, we analyzed how six projects were managed by one or more of the following agencies: DOA, DCF, ETF, DHS, DOT, and SWIB. We found that these six agencies did not consistently evaluate in writing the advantages and disadvantages of transitioning to cloud computing services provided by firms and did not consistently adhere to various best practices for data security on these projects. We provide recommendations for improvements.

Policies

DOA established few policies that specifically address how state agencies are to acquire cloud computing services from firms.

As noted, statutes require DOA to cooperate with state agencies to establish policies for administering IT services. We found that DOA established few policies that specifically address how agencies are to acquire cloud computing services from firms. The policies that DOA did establish require it to collaborate with agencies to determine when to use cloud computing services provided by firms, based on factors such as liability, regulatory compliance, risk, and cost. However, the policies do not specify whether they apply to certain entities that operate with greater statutorily prescribed autonomy from DOA than most agencies. For example, it is unclear whether the policies apply to SWIB or the Wisconsin Economic Development Corporation. DOA indicated that such entities themselves determined whether the policies apply to them.

We found that DOA's policies do not require state agencies to evaluate in writing the advantages and disadvantages of contracting

with such firms, as opposed to relying on services provided by DOA's data center, when both options are available. Such evaluations are particularly important when projects involve significant expenditures and sensitive data. For example, DHS did not evaluate in writing the advantages and disadvantages of contracting with a firm when implementing its cloud computing-based Electronic Health Records project. This project is budgeted to cost $33.0 million and involves information protected under the federal Health Insurance Portability and Accountability Act (HIPAA). Through February 2020, DHS spent $17.9 million on this project.

DOA should modify its policies for acquiring cloud computing services from firms, including by specifying the entities to which the policies apply. Its policies should require state agencies to evaluate in writing the advantages and disadvantages of contracting with such firms. Doing so will help to ensure agencies spend funds appropriately and help to keep the State's data secure.

☑ Recommendation

We recommend the Department of Administration:

- *modify its policies for acquiring cloud computing services from firms, including by specifying the entities to which the policies apply and requiring state agencies to evaluate in writing the advantages and disadvantages of contracting with such firms; and*

- *report to the Joint Legislative Audit Committee by January 15, 2021, on the status of its efforts to implement this recommendation.*

Only 13 of 31 state agencies indicated that they had policies and procedures governing the procurement and management of cloud computing services provided by firms.

As noted, 31 state agencies responding to our survey indicated that they used cloud computing services provided by firms. Only 13 of these 31 agencies (41.9 percent) indicated that they had policies and procedures governing the procurement and management of such services. Most of these 13 agencies indicated that their policies and procedures:

- specified who must approve the use of such services;

- specified the conditions in which sensitive data may be stored by such firms;

- required standard contractual terms regarding data security;

- required standard contractual terms ensuring that the State retains ownership of data stored by such firms; and

- required security or risk assessments before using services provided by such firms.

Less than one-half of these 13 state agencies indicated that their policies and procedures required them to consider the services provided by DOA before using cloud computing services provided by firms or to conduct cost-benefit analyses before using services provided by such firms. Similarly, less than one-half indicated that their policies and procedures specified requirements for successfully managing a migration to cloud computing services provided by firms.

In response to our requests, DCF, DHS, and SWIB did not provide us with any policies that specifically address how they are to acquire cloud computing services provided by firms. In contrast, DOT provided detailed policies that require it to ensure firms store its data at U.S. facilities, encrypt its data, notify it of data breaches, pay all expenses resulting from data breaches, and implement data security plans. ETF's policies have fewer requirements but require firms to provide it with details about their data security practices.

Projects

We reviewed six projects involving firms that provided cloud computing services. The six projects began from FY 2014-15 through FY 2019-20 and included:

- DOA's Microsoft Office 365 Preparation, which established the computing environment that enables state agencies to implement cloud-based office productivity software;

- SWIB's Charles River Development Upgrade, which upgraded a system for executing securities trades;

- DHS's Electronic Health Records, which is expected to store patient data at all seven DHS care facilities;

- ETF's Enterprise Content Manager, which is expected to enable document scanning and electronic storage of forms submitted to ETF;
- DOT's Oversize-Overweight Permitting System Upgrade, which is expected to upgrade a system that enables DOT to issue permits to oversize and overweight vehicles that use state highways; and
- DCF's Youth Assessment and Screening Instrument, which is expected to enable DCF to assess the probability that juveniles who have committed offenses will commit additional offenses and determine the service needs of juveniles who have committed offenses.

Three of the six cloud computing projects we reviewed were reported as large, high-risk IT projects.

As shown in Table 5, two of the six projects were completed, and the other four projects were ongoing at the time of our fieldwork. Three of the six projects were reported as large, high-risk IT projects. DOA's Microsoft Office 365 Preparation, SWIB's Charles River Development Upgrade, and DCF's Youth Assessment and Screening Instrument were not reported as large, high-risk IT projects.

Table 5

State Agency Cloud Computing Projects Reviewed

	State Agency	Information Provided by State Agencies: Start Date	Completion Date	Expenditures[1]
Completed Projects			**Actual**	
Microsoft Office 365 Preparation[2]	DOA	March 2015	Sept. 2016	—[3]
Charles River Development Upgrade[2]	SWIB	Oct. 2017	Oct. 2018	$ 6,056,800
Ongoing Projects			**Estimated**	
Electronic Health Records	DHS	July 2014	June 2021	33,000,000
Enterprise Content Manager	ETF	Dec. 2019	June 2021	1,900,000
Oversize-Overweight Permitting System Upgrade	DOT	Aug. 2018	Aug. 2021	1,250,000
Youth Assessment and Screening Instrument[2]	DCF	Mar. 2019	Sept. 2021	920,100

[1] Includes ongoing operational expenditures for some projects.

[2] These projects were not reported as large, high-risk IT projects.

[3] DOA did not provide expenditure information for this project.

We assessed the extent to which state agencies incorporated into these six projects various cloud computing-related best practices identified by expert groups. These include best practices for procuring cloud computing services, including by contractually requiring firms that provide such services to secure the State's data.

Needs Assessment and Procurement

State agencies did not consistently evaluate in writing the advantages and disadvantages of transitioning to cloud computing services provided by firms.

The federal General Services Administration recommends evaluating the advantages and disadvantages of transitioning to cloud computing services provided by firms. We found that three state agencies evaluated in writing the advantages and disadvantages of transitioning to cloud computing services provided by firms, but three other agencies did not do so. For example:

- ETF evaluated whether to use DOA's computing resources or to contract with a firm, and it determined that a firm would provide better services at a lower cost;

- DOA evaluated whether to use its own resources or contract with a firm, and it determined that a firm could provide office productivity services on devices other than desktop and laptop computers and require less DOA staff time to administer such services;

- SWIB evaluated whether to use its own computing resources or contract with a firm, and it determined that a firm would cost more but would provide services quicker and with more frequent upgrades;

- DCF and DHS indicated that they conducted but did not document evaluations; and

- DOT indicated that it did not conduct an evaluation because the firm that provided the software for its oversize-overweight permitting system required it to transition to cloud computing services if it wanted to continue working with the firm.

Data Security

State agencies did not consistently follow best practices for data security when completing projects involving cloud computing services provided by firms.

We found that state agencies did not consistently follow best practices for data security when completing projects involving cloud computing services provided by firms. As part of our evaluation, we examined the contracts and other documentation that agencies provided us for the six projects we reviewed.

In October 2018, DOA established policies that require state agencies to conduct security assessments before contracting with firms that provide IT services, including cloud computing services. Agencies are to assess the data security and vulnerability of such firms and the potential risk to agency operations. We found that:

- two agencies conducted security assessments before contracting with firms; and

- four agencies did not conduct security assessments before contracting with such firms, including three that contracted with the firms before DOA established its October 2018 policy.

The Center for Digital Government, which is a national research and advisory institute on IT policies and best practices in state and local government, recommends government entities contractually require firms that provide cloud computing services to annually submit data security audits. Such audits indicate whether firms have effective IT security and identify any deficiencies or concerns. We found that:

- four agencies contractually required the firms to submit annual data security audits, but three of the four did not document their reviews of the submitted audits and the fourth had not yet received such an audit because it executed its contract with the firm in December 2019; and

- two agencies did not contractually require the firms to submit such audits, including one agency that did not do so because the firm indicated it had a data security certification from an international standards organization. This certification is an acceptable alternative to ensure data security, but the firm was not contractually required to maintain it. The second agency contractually required the firm to maintain certification through a federal program that assesses data security but did not require the firm to document its certification.

The National Association of State Chief Information Officers recommends states contractually require their data to be stored in the U.S. We found that:

- two agencies contractually required the firms to store their data in the U.S.;
- one agency contractually required the firm to store its data in the U.S. or Canada;
- one agency did not contractually require the firm to store its data in the U.S., although the contract states that its data are stored in the U.S.;
- one agency contractually allowed the multinational firm to store its data in any country where the firm operates; and
- one agency did not contractually require the firm to store its data in the U.S. It indicated that it would not include such a contractual provision because the European Union's data protection requirements are more stringent than those of the U.S. However, its contract does not require its data to be stored in the European Union.

The National Association of State Chief Information Officers recommends states contractually require firms that provide cloud computing services to conduct criminal background checks on their employees and subcontractors and to not hire or work with those who fail these background checks. We found that:

- five agencies contractually required the firms to conduct background checks on their employees and subcontractors; and
- one agency did not contractually require the firm to do so.

The Center for Digital Government recommends states contractually require firms that provide cloud computing services to limit employee access to data to the minimum level necessary. We found that:

- five agencies contractually required the firms to limit employee access to their data; and
- one agency did not contractually require the firm to do so because the agency indicated that its data are not sensitive.

The Center for Digital Government recommends states contractually require firms that provide cloud computing services to pay monetary penalties or assume responsibility to pay for the effects of security breaches or unauthorized disclosure of data. We found that:

- four agencies contractually required the firms to pay monetary penalties and assume such responsibility; and

- two agencies did not contractually require the firms to do so. One agency indicated that it would be difficult to require a large firm to do so, but that it would consider a security breach or unauthorized data disclosures to be a breach of contract that would enable it to collect damages.

The National Association of State Chief Information Officers recommends states contractually require firms that provide cloud computing services to notify them of security breaches or unauthorized data disclosures. We found that:

- four agencies contractually required the firms to notify them of security breaches and unauthorized data disclosures; and

- two agencies did not contractually require the firms to do so, including one agency that indicated it would be difficult to require a large firm to do so.

DOA should require state agencies, including itself, that contract with firms that provide cloud computing services to take appropriate actions to safeguard the State's data. Such actions should include:

- reviewing IT security audits of firms and documenting the results of these reviews before executing contracts;

- annually reviewing IT security audits of firms;

- contractually requiring the State's data to be stored in the U.S.;

- contractually requiring firms to conduct criminal background checks on employees and subcontractors and to not hire or work with those who fail these background checks;

- contractually requiring firms to limit access to the State's data;

- contractually requiring firms to pay monetary penalties for security breaches or unauthorized disclosure of the State's data; and

- contractually requiring firms to notify them of security breaches or unauthorized data disclosures.

☑ Recommendation

We recommend the Department of Administration:

- *require state agencies, including itself, that contract with firms that provide cloud computing services to take various appropriate actions to safeguard the State's data; and*

- *report to the Joint Legislative Audit Committee by January 15, 2021, on its efforts to implement this recommendation.*

■ ■ ■ ■

IT Security ■

Managing cybersecurity risk is critical to ensuring the State's overall IT security.

Managing cybersecurity risk is critical to ensuring the State's overall IT security. DOA is statutorily responsible for establishing policies, procedures, and processes that address the needs of state agencies and for monitoring adherence to these policies, procedures, and processes. Statutes also require DOA to ensure that all state data processing facilities develop proper privacy and security procedures and safeguards. DOA operates the primary data center used by agencies for their data and applications. We reviewed IT security at five state agencies and found a number of concerns. We recommend DOA take steps to improve IT security and report on its progress in addressing these concerns.

DOA has not submitted the report we recommended it submit to the Joint Legislative Audit Committee describing its plans and timelines to address prior IT concerns we found.

We found IT security concerns in prior audits of DOA and reported these concerns in the State of Wisconsin FY 2014-15 Financial Statements (report 16-2), the State of Wisconsin FY 2015-16 Financial Statements (report 17-4), the State of Wisconsin FY 2016-17 Financial Statements (report 18-3), and the State of Wisconsin FY 2018-19 Financial Statements (report 19-30). In report 19-30, we reported concerns about DOA's implementation of policies, standards, and procedures, as well as its monitoring of other executive branch agencies, and we recommended that DOA make improvements. Because DOA had not fully addressed our concerns over a period of years, we recommended that it report to the Joint Legislative Audit Committee by April 2020 on its plans and timeline for addressing our concerns. As of August 2020, DOA had not submitted this report. Future audits will follow up on the concerns we identified.

IT Security Concerns

State agencies retain a variety of data to administer their programs, including confidential and sensitive data such as personally identifiable information and medical records. To protect these data and ensure the continuity of operations, agencies must maintain appropriate IT security measures. These measures should form layers of defense that, when working together, protect the State's data and the applications that process these data.

NIST developed a cybersecurity framework that is intended to help entities manage and reduce cybersecurity risks.

In establishing its IT policies and procedures for state agencies, DOA indicated that it used the IT security standards and guidelines of the National Institute of Standards and Technology (NIST). NIST developed a cybersecurity framework that is intended to help entities manage and reduce cybersecurity risks, such as the risk that confidential or sensitive data may be breached or inappropriately changed, critical data may be held for ransom, and critical applications may be rendered unusable. The cybersecurity framework has been widely adopted by public and private entities throughout the nation.

NIST's cybersecurity framework identifies IT security standards, guidelines, and practices. The framework focuses on five core functions that are critical for entities such as the State to manage cybersecurity risks, including the:

- identify function, in which an entity gathers the information and knowledge it needs to determine, assess, and address risks;
- protect function, in which an entity develops and implements appropriate safeguards to reduce risks;
- detect function, in which an entity actively seeks to identify cyberattacks;
- respond function, in which an entity develops and implements appropriate action plans if a cyberattack occurs; and
- recover function, in which an entity develops and implements appropriate actions to restore data, capabilities, or services affected by a cyberattack.

DOA is responsible for maintaining the State of Wisconsin *IT Security Policy Handbook*, which became effective in October 2018. All state agencies are expected to follow the policies and standards in this handbook.

We found that IT security policies and standards were incomplete or inadequate.

We found that the policies and standards in the *IT Security Policy Handbook* did not include all anticipated elements relevant to appropriate IT security, such as requirements related to the management of IT assets. We also found that state agency-specific policies, standards, and procedures were not fully compliant with the policies and standards in the *IT Security Policy Handbook*. Incomplete or inadequate policies, standards, and procedures increase the risk that data, applications, and agency operations may not be adequately protected and could be compromised.

Our review of IT security at five state agencies found 23 concerns pertaining to four of the five core functions of the NIST cybersecurity framework.

Our high-level review of IT security at five state agencies found 23 concerns pertaining to four of the five core functions of the NIST cybersecurity framework. We found concerns at all five of the state agencies we reviewed. We also identified concerns with communication between DOA and other agencies, such as those related to the division of responsibility. This likely contributed to some of the 23 concerns identified. We determined that the detailed results of our review were too sensitive to communicate publicly. Therefore, we communicated the results in a confidential interim memorandum to DOA.

DOA should regularly review and update the *IT Security Policy Handbook* and related standards in order to ensure that they reflect current NIST standards and meet state agency needs. DOA should work with agencies to address each of the 23 IT security concerns that we found. DOA should also ensure that all agencies, including itself, comply with the *IT Security Policy Handbook*. To help ensure this occurs, DOA should report to the Joint Legislative Audit Committee on its efforts to improve IT security in the core functions of NIST's cybersecurity framework. When doing so, it should refrain from providing details that could potentially harm IT security at state agencies. In future audits, we will continue to monitor the extent to which DOA has implemented our recommendations.

☑ Recommendation

We recommend the Department of Administration;

- *regularly review and update the IT Security Policy Handbook and related standards in order to ensure that they reflect current National Institute of Standards and Technology standards and meet state agency needs;*

- *work with state agencies to address each of the 23 information technology security concerns that we found;*

- *ensure all state agencies, including itself, comply with the IT Security Policy Handbook;*

- *immediately submit to the Joint Legislative Audit Committee the report that was due in April 2020; and*

- *report to the Joint Legislative Audit Committee by November 13, 2020, on its efforts to implement these recommendations.*

Issue for Legislative Consideration

The Legislature could consider modifying statutes to allow governmental bodies to convene in closed session in order to discuss IT security issues.

Section 19.85 (1), Wis. Stats., allows meetings of governmental bodies to convene in closed session in order to discuss statutorily specified issues, such as certain personnel issues. However, statutes do not allow governmental bodies to convene in closed session in order to discuss IT security issues, such as the concerns we found during our review of IT security at five state agencies. Discussing such concerns during an open meeting would potentially compromise the security of the State's data and systems. The Legislature could consider modifying statutes to allow governmental bodies to convene in closed session in order to discuss IT security issues. Doing so would allow it to obtain detailed information about the concerns we found, question agencies about the concerns, understand actions that agencies had taken and planned to take to address the concerns, and offer guidance and support to agencies. We note that modifying statutes to allow a governmental body to meet in closed session to discuss IT security issues would not guarantee that the sensitive information discussed in such a meeting would remain confidential after such a meeting ended.

■ ■ ■ ■

Improving Oversight ■

DOA needs to improve its oversight of IT projects, including large, high-risk IT projects.

DOA needs to improve its oversight of IT projects, including large, high-risk IT projects. Statutes require DOA to ensure that state agencies make effective and efficient use of IT resources. Statutes also require DOA to establish IT policies and procedures, which agencies must follow, and monitor the adherence of agencies to these policies and procedures. DOA should consistently comply with statutory requirements pertaining to its oversight of projects, including large, high-risk IT projects, and it should help agencies to develop appropriate policies for contracting with firms that provide cloud computing services. In addition, monitoring could be improved if the Joint Committee on Information Policy and Technology met more regularly.

DOA's Oversight

We found that DOA did not consistently perform IT oversight duties that are required by statutes and its policies.

As noted, we found that DOA did not consistently perform IT oversight duties that are required by statutes and its policies, including for large, high-risk IT projects. For example, DOA:

- did not require state agencies to include all statutorily required information in their March 2019 IT strategic plans;
- did not comply with statutes because it did not submit statewide IT strategic plans to the Joint Committee on Information Policy and Technology in recent years;

- did not comply with its policies because it did not ensure that an interagency committee conducted technical reviews of large, high-risk IT projects;

- did not comply with statutes because it did not review and approve eight contracts, totaling an estimated $93.5 million, for five large, high-risk IT projects;

- did not submit any of the statutorily required semiannual reports to the Joint Committee on Information Policy and Technology from March 2014 through September 2019; and

- did not include requirements pertaining to asset management in the *IT Security Policy Handbook*.

We found that state agencies did not consistently comply with statutes, policies, and best practices for managing projects.

We found that state agencies did not consistently comply with statutes, policies, and best practices for managing projects, including large, high-risk IT projects. As noted, agencies:

- did not consistently include all projects and all statutorily required information in the IT strategic plans they submitted to DOA in recent years;

- did not include in their contracts for large, high-risk IT projects a statutorily required stipulation that DOA must approve orders and amendments that would change the contract scope and increase the contract price;

- did not consistently provide DOA with complete and accurate information about their large, high-risk IT projects from September 2014 through September 2019;

- did not consistently evaluate in writing the advantages and disadvantages of transitioning to cloud computing services provided by firms;

- did not consistently follow best practices for data security when completing projects involving cloud computing services provided by firms; and

- did not fully comply with the policies and standards in the *IT Security Policy Handbook*.

DOA should consistently comply with statutory requirements pertaining to its oversight of projects, including large, high-risk IT projects.

DOA should consistently comply with statutory requirements pertaining to its oversight of projects, including large, high-risk IT projects. As the entity that is statutorily responsible for ensuring that state agencies make effective and efficient use of IT resources and for monitoring adherence to established IT policies and procedures, DOA must also ensure that agencies consistently comply with statutory and policy requirements pertaining to projects, including large, high-risk IT projects, and IT security.

☑ Recommendation

We recommend the Department of Administration:

- *consistently comply with statutory requirements pertaining to its oversight of information technology projects;*
- *ensure that state agencies consistently comply with statutory and policy requirements pertaining to information technology projects and information technology security; and*
- *report to the Joint Legislative Audit Committee by January 15, 2021, on its efforts to implement these recommendations.*

As noted, DOA established few policies that specifically address how state agencies are to acquire cloud computing services from firms. The policies it did establish did not require agencies to evaluate in writing the advantages and disadvantages of contracting with them. In addition, few agencies indicated that they had policies and procedures governing the procurement and management of such services.

DOA should help state agencies to develop appropriate policies for contracting with firms that provide cloud computing services.

DOA should help state agencies to develop appropriate policies for contracting with firms that provide cloud computing services. Doing so will help to ensure that agencies follow best practices for procuring cloud computing services, including by contractually requiring the firms to secure the State's data. In the future, agencies may be increasingly likely to contract with such firms, which may store and have some degree of control over increasing amounts of the State's data. To the extent that these data are sensitive or confidential, it will be crucial for agencies to effectively manage their contractual relationships with the firms.

☑ **Recommendation**

We recommend the Department of Administration:

- *help state agencies to develop appropriate policies for contracting with firms that provide cloud computing services; and*

- *report to the Joint Legislative Audit Committee by January 15, 2021, on its efforts to implement this recommendation.*

Issues for Legislative Consideration

The Legislature could consider modifying statutes to focus DOA's IT oversight duties.

The Legislature could consider modifying statutes to focus DOA's IT oversight duties. Currently, statutes require DOA to review and approve all contracts for IT projects, and to approve any order or amendment that would change the contract scope and increase the contract price for large, high-risk IT projects. If DOA were instead required to approve only those contracts over a minimum dollar threshold and only those orders and amendments over a minimum dollar threshold, DOA may be able to more effectively oversee these largest contracts. Until modifications are made, DOA must comply with statutes as written and oversee all contracts for IT projects.

The Legislature could consider modifying statutes to increase the dollar threshold of a large, high-risk IT project.

The Legislature could consider modifying statutes to increase the dollar threshold of a large, high-risk IT project. 2007 Wisconsin Act 20, the 2007-09 Biennial Budget Act, established that large, high-risk IT projects include those projects that are expected to cost more than $1.0 million. As noted, the March 2020 semiannual report on large, high-risk IT projects included 19 projects that were each anticipated to cost less than $5.0 million, 6 projects that were each anticipated to cost between $5.0 million and $10.0 million, and 4 projects that were each anticipated to cost more than $10.0 million. However, the $1.0 million threshold may no longer be as relevant in 2020 for a number of reasons. Inflation has increased the cost of many items since the enactment of Act 20, and projects undertaken today may be considerably different than those that began in 2007. Modifying the statutory definition of a large, high-risk project may also help DOA to focus its oversight duties.

Statutes provide a monitoring role for the Joint Committee on Information Policy and Technology, including by receiving semiannual reports from DOA and the Board of Regents on large, high-risk IT projects. As noted, DOA did not submit any reports from March 2014 through September 2019. Although the Board of Regents did submit reports, these reports excluded information

about some ongoing large, high-risk IT projects, and the information that was included was not consistently accurate and complete.

If the Joint Committee on Information Policy and Technology met more regularly, it could monitor the status of large, high-risk IT projects.

Since the 2011-12 legislative session, the Joint Committee on Information Policy and Technology has met for informational hearings three times: in June 2015, November 2015, and March 2017. During these hearings, the Committee received information on issues related to STAR, cybersecurity, and other IT issues. If the Joint Committee on Information Policy and Technology met more regularly, it could monitor the status of large, high-risk IT projects. The Committee could ask DOA, UW System Administration, and other state agencies to explain the need for IT projects, including those including cloud computing services provided by firms. The Committee could also ask agencies to explain why project costs increased, why anticipated project completion dates changed, and how agencies planned to control future project costs.

■ ■ ■ ■

Appendix ■

Appendix

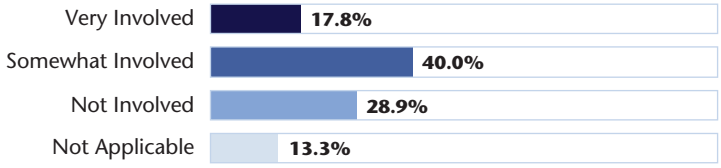
Opinions of State Agencies

In January 2020, we surveyed 45 state agencies about various issues pertaining to IT needs assessment and procurement, cloud computing, and IT security. Each agency responded to our survey, but not all responded to each survey question.

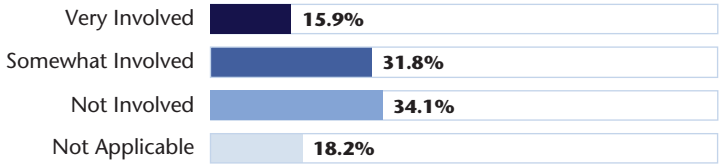
The following pages summarize the responses of state agencies to our survey.

DOA's Involvement with Selected IT Tasks at State Agencies[1]

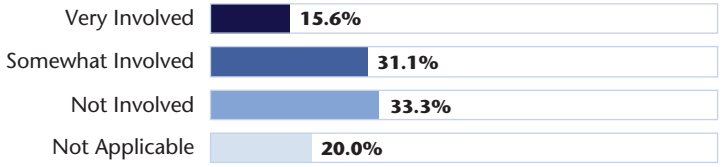
Assessing the Need for New or Improved IT Products



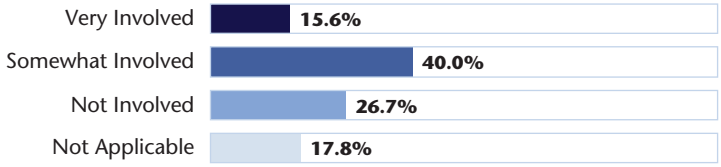
Conducting Cost-Benefit Analyses of Proposed IT Products



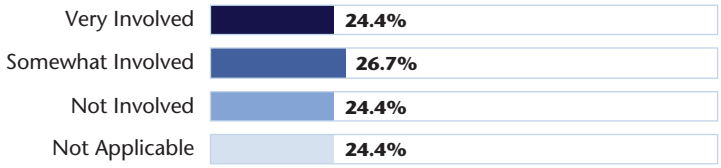
Assessing Commercially Available Off-the-Shelf IT Products



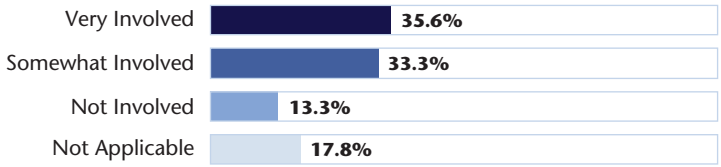
Assessing Whether IT Products or Contracts at Other State Agencies Could Meet an Agency's Needs



Developing Procurement Plans and Solicitations



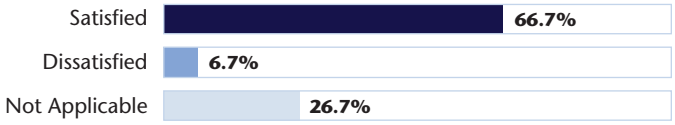
Developing or Negotiating Contracts with IT Vendors



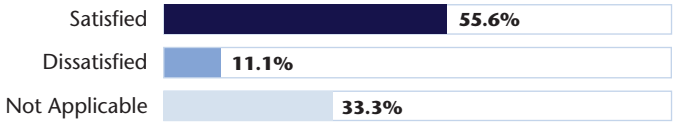
[1] According to survey respondents.

Satisfaction with DOA's Involvement with Selected IT Tasks[1]

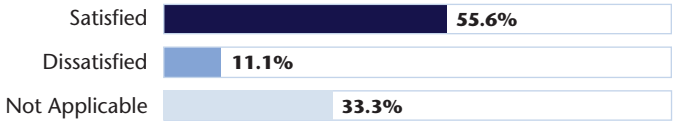
Assessing the Need for New or Improved IT Products



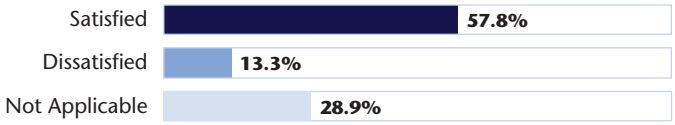
Conducting Cost-Benefit Analyses of Proposed IT Products



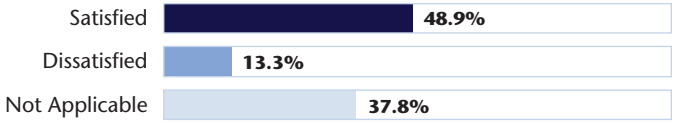
Assessing Commercially Available Off-the-Shelf IT Products



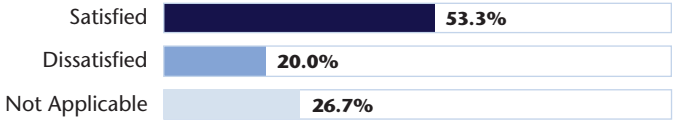
Assessing Whether IT Products or Contracts at Other State Agencies Could Meet an Agency's Needs



Developing Procurement Plans and Solicitations

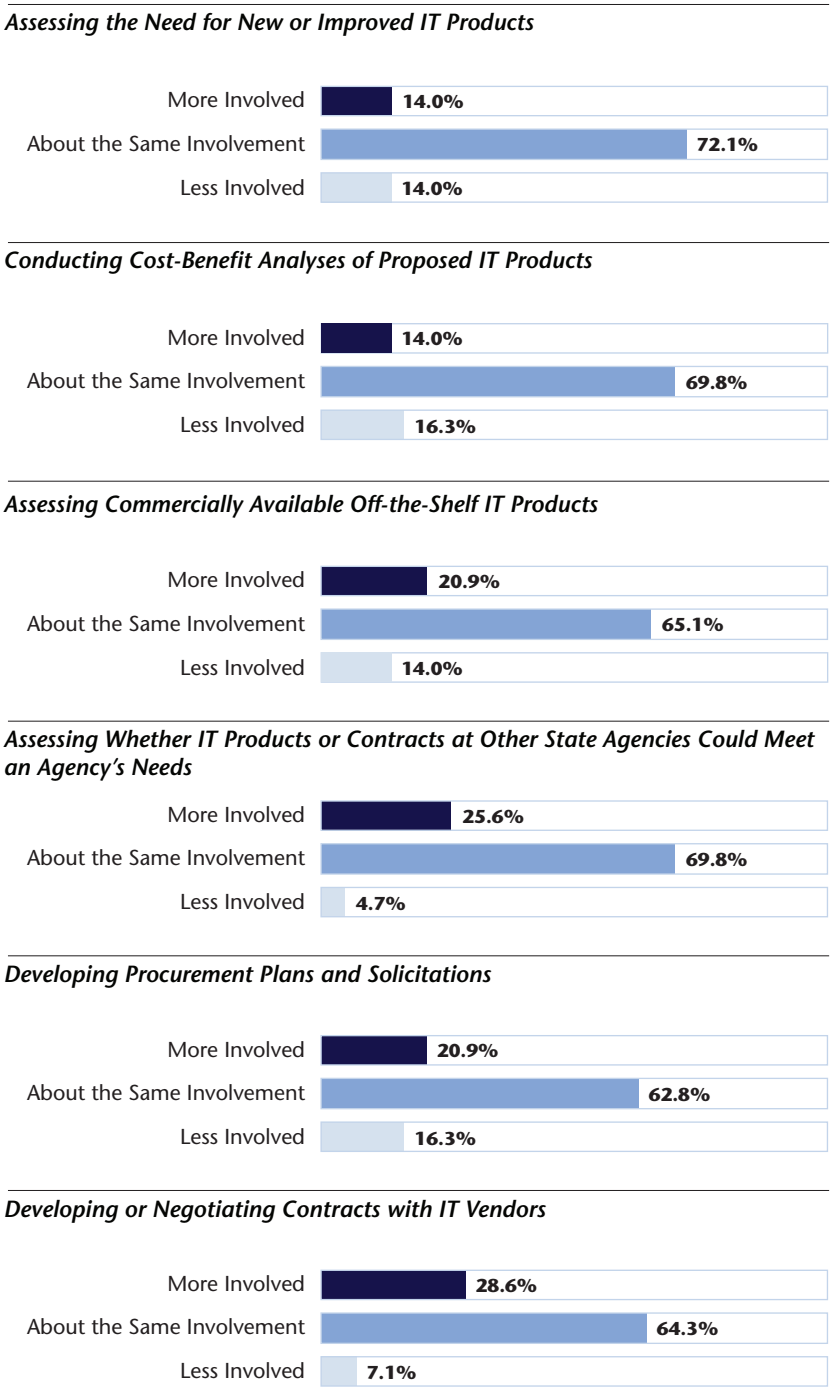


Developing or Negotiating Contracts with IT Vendors



[1] According to survey respondents.

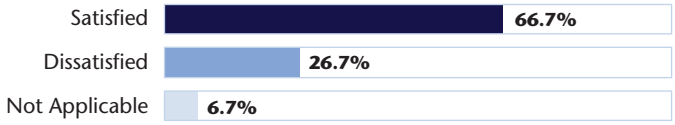
State Agencies' Preferred Level of Involvement of DOA with Selected IT Tasks[1]



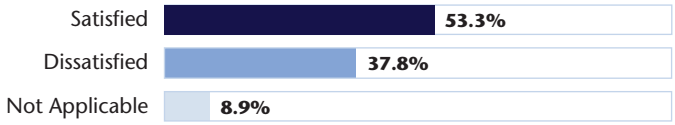
[1] As indicated by survey respondents.

Satisfaction of State Agencies with the Enterprise IT Products Provided by DOA[1]

Types of Products



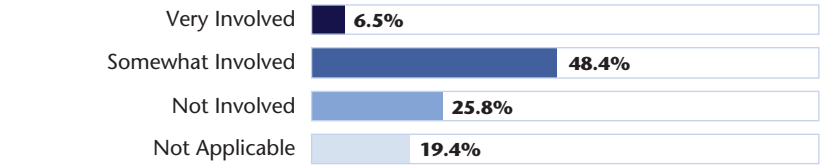
Quality of Products



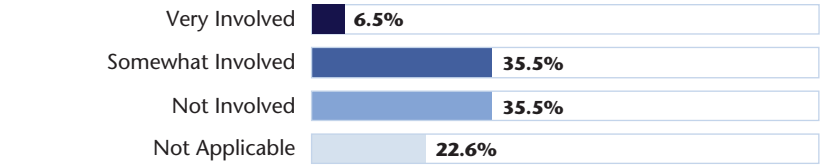
[1] As indicated by survey respondents.

DOA's Involvement in Helping State Agencies with Selected Cloud Computing Tasks[1]

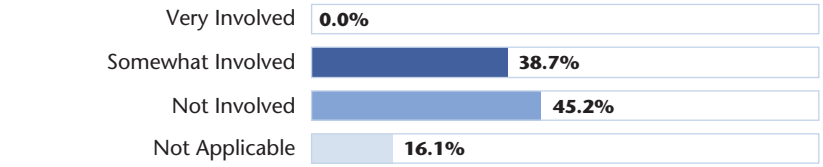
Identifying Services Provided by DOA That Could Serve as Alternatives to Cloud Computing Services Provided by Firms



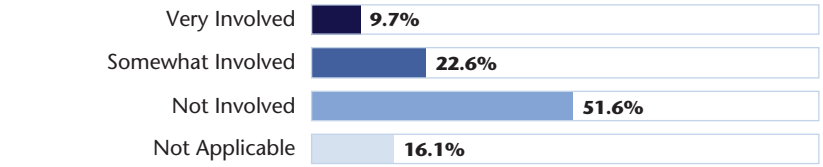
Developing Procurement Plans and Solicitations for Cloud Computing Services



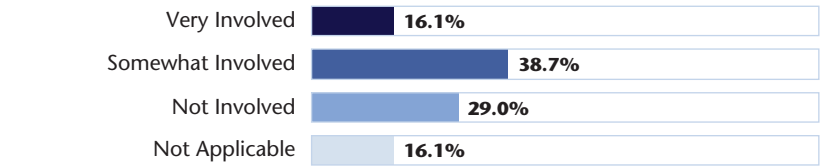
Evaluating the Quality of Cloud Computing Services Provided by Potential Vendors



Conducting Security and Risk Assesments of Cloud Computing Services Provided by Firms



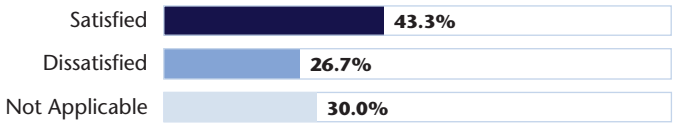
Developing and Negotiating Contracts with Firms That Provide Cloud Computing Services



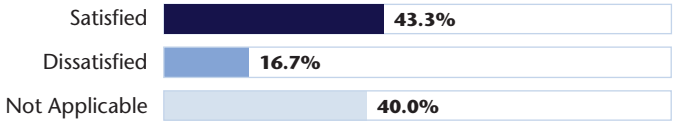
[1] As indicated by survey respondents.

Satisfaction of State Agencies with the Involvement of DOA with Selected Cloud Computing Tasks[1]

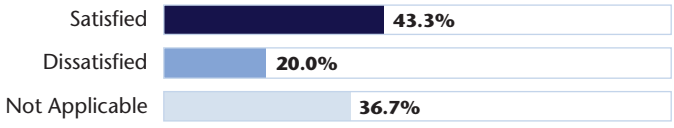
Identifying Services Provided by DOA That Could Serve as Alternatives to Cloud Computing Services Provided by Firms



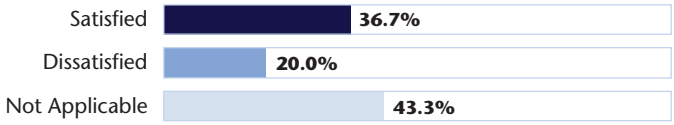
Developing Procurement Plans and Solicitations for Cloud Computing Services



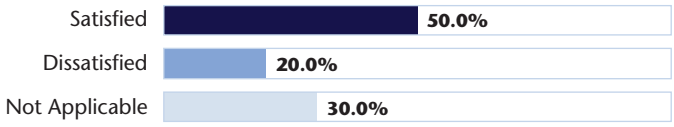
Evaluating the Quality of Cloud Computing Services Provided by Potential Vendors



Conducting Security and Risk Assessments of Cloud Computing Services Provided by Firms

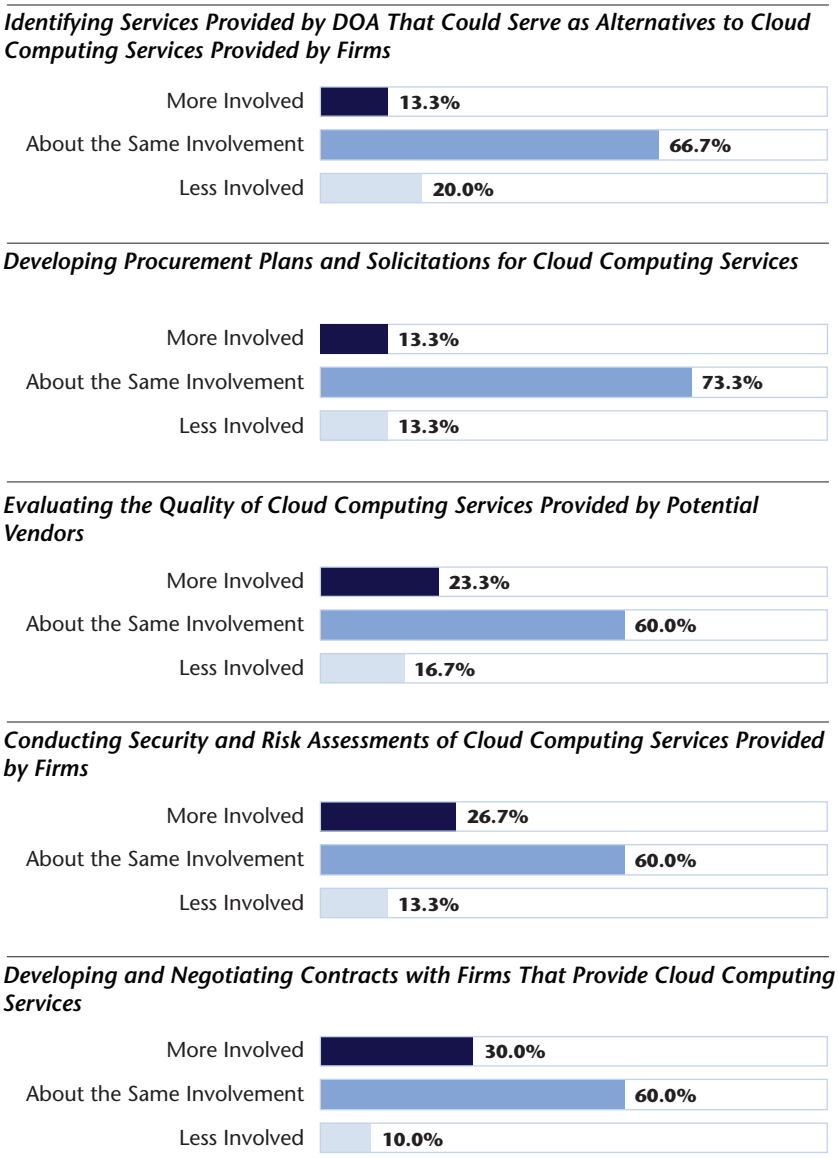


Developing and Negotiating Contracts with Firms That Provide Cloud Computing Services



[1] As indicated by survey respondents

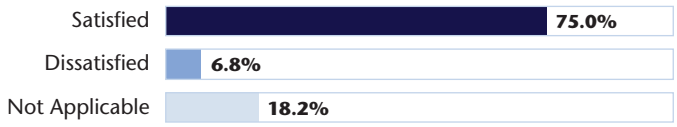
State Agencies' Preferred Level of Involvement of DOA with Selected Cloud Computing Tasks[1]



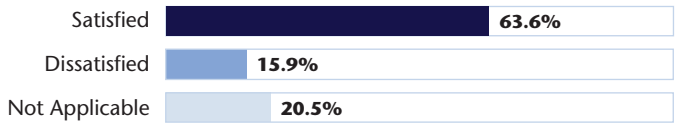
[1] As indicated by survey respondents.

Satisfaction of State Agencies with Selected IT Security Services Provided by DOA[1]

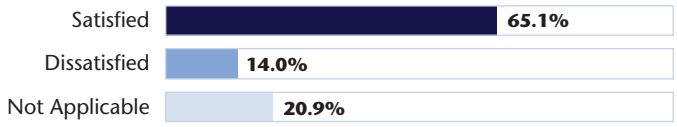
IT Security Policy Development



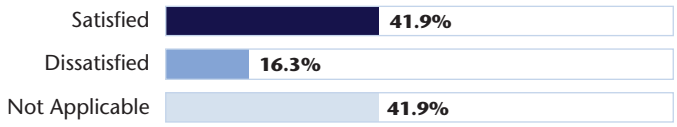
IT Security Policy Implementation



IT Security at DOA's Data Center



IT Security of Firms Managed by DOA

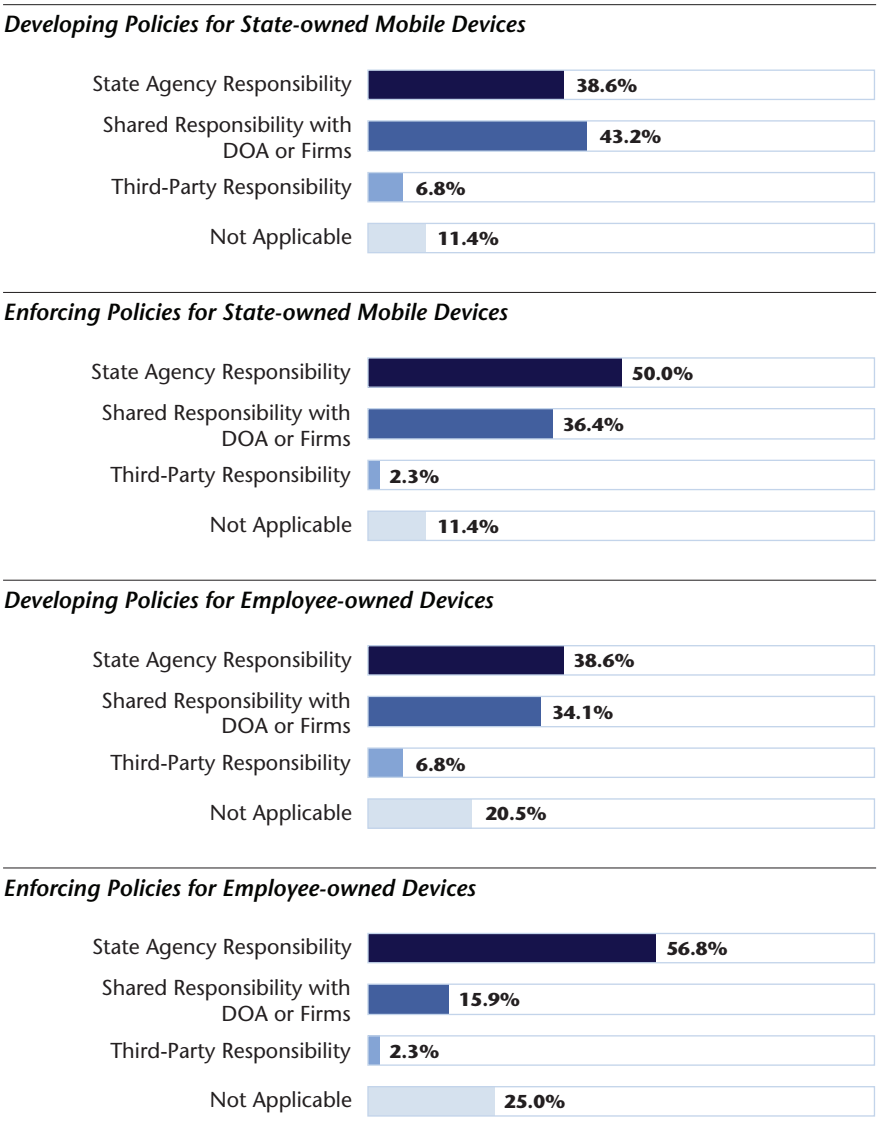


[1] As indicated by survey respondents.

Extent to which State Agencies Communicated Their Data Classifications and Had Security Agreements[1]

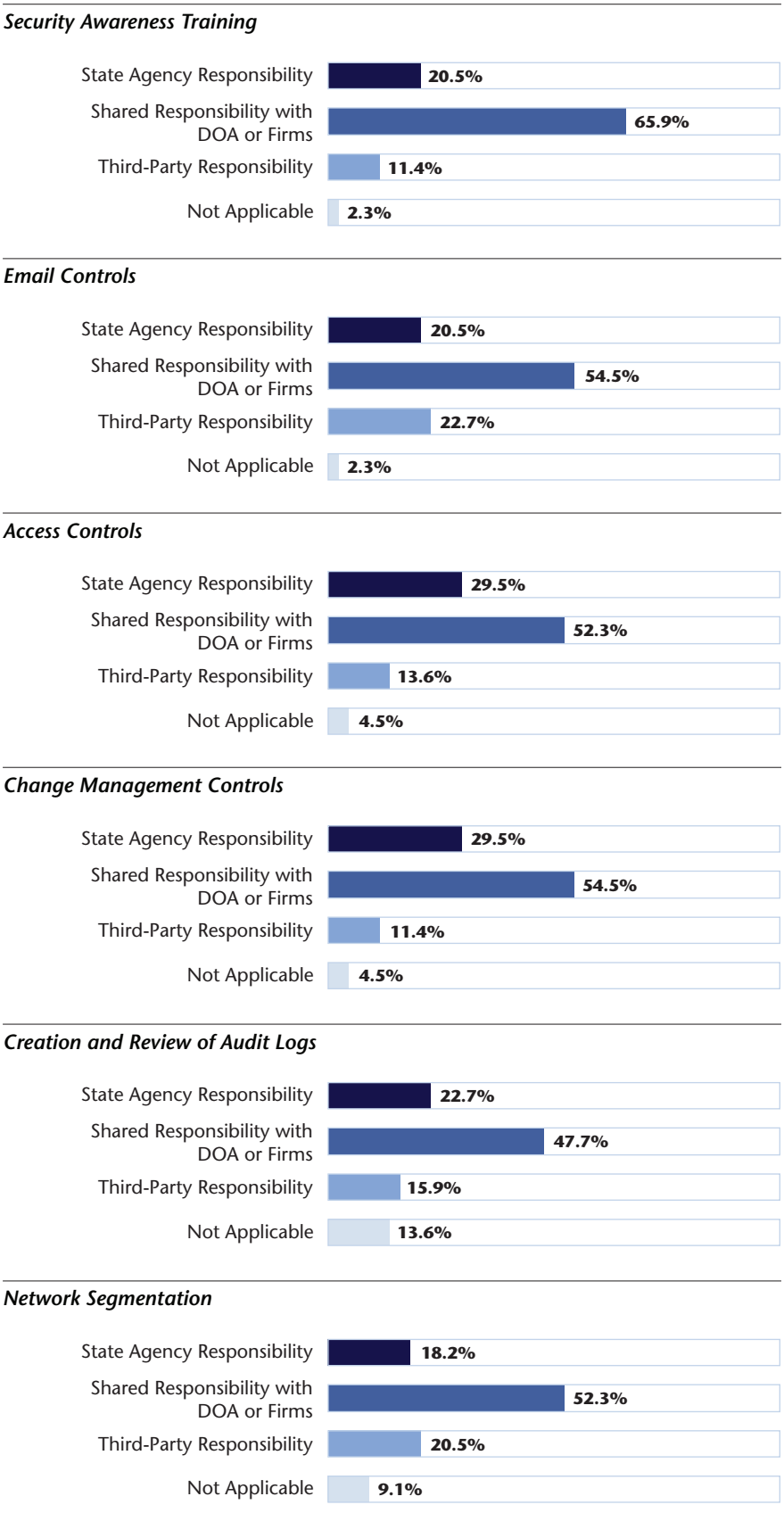
[1] As indicated by survey respondents. Percentages do not total to 100.0 percent because survey respondents could provide multiple answers.

Who Has Responsibility for Developing and Enforcing Policies for Mobile Devices[1]



[1] As indicated by survey respondents.

Who Has Responsibility for Selected Aspects of IT Security[1]



[1] As indicated by survey respondents.

Response ■

STATE OF WISCONSIN
DEPARTMENT OF ADMINISTRATION
Tony Evers, Governor
Joel Brennan, Secretary

August 28, 2020

Joe Chrisman, State Auditor
Legislative Audit Bureau
22 East Mifflin Street, Suite 500
Madison, WI 53703

Dear Mr. Chrisman:

On behalf of the Department of Administration (DOA), I would like to thank the Legislative Audit Bureau for its evaluation of the State's information technology (IT) needs assessment and procurement processes. DOA greatly appreciates the work and the consideration provided to us and the other agencies in the development of the report.

DOA is committed to addressing IT issues across state government. We plan to use your recommendations in following state statutes and policies and fulfilling our legislative reporting requirements as the foundation for future improvements. The Department will work collaboratively with other state agencies to ensure the recommendations made in the report are implemented.

The Department has already taken steps to address some of the concerns identified in the report based on an internal review of our statutory responsibilities. We recently implemented changes consistent with your recommendations to the Agency Annual IT Strategic Plans process, the Statewide IT Strategic Plan process, the submissions of various reports for these items, along with the large, high-risk project reporting. For other findings, we will ensure we have proper corrective action plans in place to fully address the recommendations and will be making assignments to key people within our organization to address these concerns in a timely manner. The Department will document these and other compliance efforts in a report to the Joint Legislative Audit Committee (JLAC) by January 15, 2021.

The Department has also begun work to address concerns related to IT security. We have already established an annual review of the IT Security Policy Handbook and related standards and will ensure the process exhibits current National Institute of Standards and Technology standards while also addressing specific agency security needs and controls. The Department will work with agencies to address each of the IT security concerns found in the report and develop plans for ensuring compliance with the IT Security Policy Handbook and related standards. The Department will report to the JLAC on its efforts to implement the auditors' IT security recommendations by November 13, 2020 as recommended. Further, the Department will provide the report to JLAC that was due April 2020 under separate cover.

Thank you again for your time and consideration in completing this report. I appreciate the opportunity to comment on your findings and recommendations. I look forward to strengthening the State's management and oversight of IT projects and initiatives as an outcome of this report.

Sincerely,

Joel Brennan

Joel T. Brennan
Secretary