IT Needs Assessment, Procurement, and Security

Report 20-10: University of Wisconsin System

Report 20-11: Department of Administration

Report 20-12: Master Lease Program

September 2020

Report Highlights

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.

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.

UW System

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.

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. 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. 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.

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, 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, 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*).