



IT Needs Assessment, Procurement, and Security

Department of Administration

Background

The Department of Administration (DOA) is statutorily responsible for ensuring that executive branch agencies, other than the University of Wisconsin (UW) System, make effective and efficient use of information technology (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.

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.

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 also analyzed [IT security](#) at a different set of five agencies.

Key Findings

- [The table](#) summarizes our key audit findings, including those that pertain to needs assessment and planning, procurement, project reporting, cloud computing, and IT security.
- State agencies did not consistently comply with various statutes, policies, and best practices.
- We identified concerns with IT security at five state agencies and conveyed these concerns to DOA, which is responsible for monitoring agency adherence to its IT policies and procedures.
- DOA needs to improve its oversight of IT projects.

Recommendations

[We recommend](#) DOA:

- improve IT needs assessment and procurement, including on projects involving cloud computing services provided by firms;
- work with state agencies to improve IT security; and
- improve oversight by complying with statutory requirements and helping state agencies to develop appropriate policies for contracting with firms that provide cloud computing services.

In addition, the [Legislature could consider](#) modifying statutes to allow governmental bodies to convene in closed session in order to consider IT security issues, focus DOA's oversight duties, and increase the dollar threshold of a large, high-risk IT project.

Continued on next page

Key Audit Findings for DOA

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).

[View Highlights for Report 20-11](#)