Report 20-10
September 2020

IT Needs Assessment, Procurement, and Security

University of Wisconsin System

State of Wisconsin



Legislative Audit Bureau

Report 20-10
September 2020

IT Needs Assessment, Procurement, and Security

University of Wisconsin System

Joint Legislative Audit Committee Members

Senate Members:

Robert Cowles, Co-chairperson
Chris Kapenga
Alberta Darling
Janet Bewley
Tim Carpenter

Assembly Members:

Samantha Kerkman, Co-chairperson
John Macco
John Nygren
Melissa Sargent
Katrina Shankland

Report 20-10
September 2020

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.*

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

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 University of Wisconsin (UW) System 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 UW institutions.

The Board of Regents is responsible for overseeing IT projects in UW System. Statutes permit UW institutions to implement only those IT projects that have been approved by the Board of Regents.

We found that UW institutions, including UW System Administration, did not consistently comply with various statutes and policies pertaining to IT projects, including large, high-risk IT projects. We found that UW System Administration and UW-Madison implemented projects before obtaining the statutorily required approval from the Board of Regents, and UW institutions 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 UW institutions and have conveyed our specific concerns to UW System Administration, which should take action to address them.

The Board of Regents needs to improve its oversight of IT projects, including by modifying its policies to require UW institutions to obtain its approval to execute all IT contracts of more than $1.0 million. UW System Administration should work with the Board of Regents to establish an IT projects committee that could ensure that UW institutions consistently comply with statutes, policies, and best practices. We make a number of other recommendations for improvements.

We appreciate the courtesy and cooperation extended to us by UW System. A response from the UW System Interim President 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 ■

The Board of Regents is statutorily responsible for establishing the policies necessary for governing UW System.

Under s. 36.09 (1) (a), Wis. Stats., the Board of Regents is responsible for establishing the policies necessary for governing UW System, which includes 13 four-year universities, 13 two-year branch campuses, and UW System Administration. Membership of the 18-member Board of Regents includes 14 citizens, 2 students, the State Superintendent of Public Instruction, and the President of the Wisconsin Technical College System Board, or his or her designee. Citizen and student members are appointed by the Governor and confirmed by the Senate. Citizen members are appointed for staggered seven-year terms, and student members are appointed for two-year terms. At least one citizen member must reside in each of the State's congressional districts.

Statutes require the Board of Regents to appoint the UW System President and the chancellors of 13 UW institutions. UW System Administration, which is also a UW institution, includes the UW System President's staff who help the Board of Regents establish and monitor systemwide policies and maintain fiscal control. The UW System President and the chancellors are responsible for implementing policies established by the Board of Regents. Chancellors work under the direction of the UW System President and the Board of Regents.

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

The Board of Regents is responsible for overseeing IT projects in UW System. Statutes indicate that the Board of Regents must require each UW institution to annually submit to it a strategic plan for using IT in the next fiscal year. Statutes require these plans to identify all proposed IT projects. Board of Regents policies require

UW System Administration to coordinate and prepare these plans for the Board of Regents. Statutes require the Board of Regents to approve or disapprove of these plans by June 15. Statutes indicate that UW institutions are permitted to implement only those IT projects that have been approved by the Board of Regents.

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, and that a project is high-risk if failure to complete it on time or on budget would prevent a UW institution from running enterprise-wide IT systems or fulfilling the essential missions of instruction, research, extended training, or public service for 10 days or more. The policies also indicate that all such projects are managed and monitored by UW System Administration, which is required to review plans for these projects before their implementation and to monitor the implementation of these projects.

DOA has statutorily defined responsibilities for IT security in state agencies. Statutes require DOA to ensure that all state data processing facilities develop proper privacy and security procedures and safeguards, to use all feasible technical means to ensure the security of all information submitted to it by agencies for processing, and to establish policies, procedures, and processes that address the needs of agencies and monitor adherence to these policies, procedures, and processes. UW System manages IT security for UW institutions.

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 UW System, which is statutorily permitted to manage its IT projects separate from other state agencies. In report 20-11, we considered these issues in other state agencies. In report 20-12, we considered DOA's management of the master lease program that agencies, including UW System, can use to fund IT and other types of projects.

We previously conducted evaluations that analyzed UW System'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. In addition, we analyzed IT security issues in our financial audits of UW System for fiscal year (FY) 2012-13 (report 14-3), FY 2013-14 (report 15-1), FY 2014-15 (report 16-3), FY 2015-16 (report 17-6), and FY 2016-17 (report 18-2), as well as in our *State of Wisconsin FY 2017-18 Single Audit* (report 19-3).

To complete this evaluation, we analyzed how five UW institutions—UW System Administration, UW-Eau Claire, UW-Madison, UW-Milwaukee, and UW-Stevens Point—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. 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 UW-Madison provided to UW institutions through its data center. Finally, we reviewed IT security at a different set of five UW institutions. A comprehensive evaluation of the costs of IT projects or the management of individual IT projects by UW institutions was not in the scope of this evaluation.

In January 2020, we surveyed every UW institution except for UW System Administration about IT needs assessment and procurement, cloud computing, and IT security issues.

In January 2020, we surveyed every UW institution except for UW System Administration about IT needs assessment and procurement, cloud computing, and IT security issues. Every UW institution responded to our survey and indicated that it 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 of UW institutions.

We did not receive all information that we requested from UW System Administration. In January 2020, we requested that UW System Administration provide planning documents and contracts pertaining to projects we reviewed. Although we restated our January 2020 information request in February 2020, March 2020, and April 2020, we did not receive all requested information or an explanation of why it could not be provided. As a result, we were unable to fully assess contractual obligations pertaining to five projects we reviewed.

■ ■ ■ ■

IT Needs Assessment and Procurement ■

We evaluated how UW System assessed its IT needs and procured goods and services for projects.

We evaluated how UW System assessed its IT needs and procured goods and services for projects. To do so, we reviewed 10 projects managed by one or more of the following UW institutions: UW System Administration, UW-Eau Claire, UW-Madison, UW-Milwaukee, and UW-Stevens Point. We found that UW institutions began projects before obtaining the necessary statutory approval from the Board of Regents, did not consistently comply with statutes and Board of Regents policies when executing contracts, and did not consistently comply with statutory requirements when reporting information to the Board of Regents about projects. We make a number of recommendations to UW System Administration for improvements.

Projects

The 10 projects we reviewed began from FY 2013-14 through FY 2018-19 and included:

- UW System Administration's Shared Financial System Upgrade, which upgraded the software that operates UW System's financial database;

- UW System Administration's Human Capital Management Upgrade, which upgraded UW System's Human Resource System (HRS) that contains personnel, payroll, and benefits processing information;

- UW System Administration's Student Information System Restructuring, which transferred student data from two-year institutions to four-year institutions as part of UW System's restructuring;
- UW-Stevens Point's Student Information System Implementation, which replaced a legacy system with the system used by other UW institutions;
- UW System Administration's Interactive Reporting Tool Replacement, which created a single reporting platform for various data;
- UW-Madison's Canvas Transition, which implemented a learning management system;
- UW-Madison's Student Information System Upgrade, which upgraded the system for managing student data;
- UW-Milwaukee's Microsoft Office 365 Preparation, which replaced UW-Milwaukee's legacy email and calendar system;
- UW-Eau Claire's Student Success Collaborative, which implemented a management system to provide data-based interventions and proactive student support; and
- UW System Administration's Student Success Collaborative, which is expected to implement a management system to provide data-based interventions and proactive student support.

Nine of the 10 projects we reviewed were reported as large, high-risk IT projects.

As shown in Table 4, 9 of the 10 projects we reviewed were completed, and 1 project was ongoing at the time of our fieldwork. UW institutions reported that 9 of the 10 projects were large, high-risk IT projects. UW-Eau Claire reported that the Student Success Collaborative project was not a large, high-risk IT project.

Table 4

UW System IT Projects Reviewed

		Information That UW Institutions Reported to the Board of Regents		
	UW Institution	Start Date	Completion Date	Expenditures
Completed Projects			**Actual**	
Shared Financial System Upgrade	System Administration	May 2017	Nov. 2018	$7,913,200
Human Capital Management Upgrade	System Administration	Jan. 2016	Nov. 2017	7,526,800
Student Information System Restructuring	System Administration	May 2018	Oct. 2019	6,187,400
Student Information System Implementation	Stevens Point	Jan. 2016	Sept. 2018	5,092,600
Interactive Reporting Tool Replacement	System Administration	Dec. 2015	Feb. 2019	4,831,900
Canvas Transition	Madison	July 2017	June 2019	4,490,000
Student Information System Upgrade	Madison	June 2018	July 2019	3,424,700
Microsoft Office 365 Preparation	Milwaukee	Aug. 2013	Jan. 2015	146,100
Student Success Collaborative[1]	Eau Claire	–	–	–
Ongoing Project			**Estimated**	
Student Success Collaborative	System Administration	Jan. 2019	Nov. 2020	10,700,000

[1] UW-Eau Claire was not required to report certain information about this project, which was not reported as a large, high-risk IT project, and could not locate this information for us.

Needs Assessment and Planning

Statutes require UW institutions to complete an annual IT strategic plan that contains certain information about all proposed projects.

Statutes require UW institutions to complete an annual IT strategic plan that contains certain information about all proposed projects. Board of Regents policies require UW institutions to complete planning documents, including a project charter and a project plan, for each large, high-risk IT project. These planning documents must contain a clear business case for a project, as well as a project's timeline, cost, and objectives. Completing IT strategic plans and planning documents helps UW institutions appropriately assess the need for projects and plan for them.

Statutes require an IT strategic plan to include information about all proposed projects that address the business needs of a given UW institution, 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. Statutes require these plans to be submitted to the Board of Regents by each March 1.

UW institutions submit their IT strategic plans to UW System Administration, which compiles the information, includes information on projects it manages, and provides one overall plan to the Board of Regents. We reviewed the plans that each UW institution submitted for March 2020 and found that they contained the statutorily required information for the projects in these plans.

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.

We found that the overall IT strategic plan that UW System Administration provided to the Board of Regents for March 2020 did not consistently include statutorily required information about each project's priority and whether a given project could be undertaken with available resources or would require additional resources. The plan contained summary information about the need and justification for each project, but it excluded the more-detailed information that UW institutions had submitted in their plans. UW System Administration informed us that it decided to provide the Board of Regents with concise information, and that annual IT strategic plans are an outdated form of management.

UW System Administration should comply with statutes by including in the annual IT strategic plan it provides to the Board of Regents all statutorily required information about all projects proposed by UW institutions. This information will allow the Board of Regents to assess the need, anticipated benefits, and priority for various projects, as well as the ability to pay for such projects, and make informed decisions about whether to approve or reprioritize projects.

☑ Recommendation

We recommend the University of Wisconsin System Administration:

- *comply with statutes by including in the annual information technology strategic plan it provides the Board of Regents all statutorily required information about all projects proposed by University of Wisconsin institutions; and*

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

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.

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. We found that:

- UW System Administration left blank several sections of the planning document for the Interactive Reporting Tool Replacement;

- UW System Administration indicated that it did not develop a clear business case for its Student Success Collaborative because most of the work to implement this project occurred at other UW institutions; and

- UW-Stevens Point indicated that it only partially completed a planning document for its Student Information System Implementation, in part, because of budget and staffing shortages.

Sufficient project planning can help to ensure that the costs of large, high-risk IT projects are estimated accurately. For example, the Interactive Reporting Tool Replacement cost $5.0 million, which was $1.2 million more than initially expected, in part because UW System Administration had not realized that UW institutions did not have the expertise to implement this project without additional assistance.

☑ Recommendation

We recommend the University of Wisconsin System Administration:

- *ensure that University of Wisconsin institutions, including itself, consistently comply with Board of Regents policies by including all required information in planning documents before implementing large, high-risk information technology projects; and*

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

Project Approval

From FY 2013-14 through FY 2019-20, the Board of Regents did not reject any annual IT strategic plans or disapprove of any projects in the plans or semiannual reports.

By each March 1 and September 1, statutes require the Board of Regents to submit to the Joint Committee on Information Policy and Technology a semiannual report with information on each project that has an actual or expected cost of more than $1.0 million or is a large, high-risk IT project. UW System Administration prepares and provides these semiannual reports to the Board of Regents before submitting them to the Committee. UW System Administration indicated that when the Board of Regents approves a semiannual report or an annual IT strategic plan, it has approved all projects in a given report or plan, unless it indicates otherwise. UW System Administration indicated that the Board of Regents did not reject any annual IT strategic plan or disapprove of any projects in the plans or semiannual reports during the seven-year period from FY 2013-14 through FY 2019-20.

UW System Administration and UW-Madison implemented projects before obtaining the statutorily required approval from the Board of Regents to do so.

Although statutes permit UW institutions to implement only those projects approved by the Board of Regents, we found that UW System Administration and UW-Madison implemented projects before obtaining such approval. For example:

- UW System Administration executed five contracts totaling $2.9 million for the Student Information System Restructuring beginning in April 2018 but first reported this project to the Board of Regents in the September 2018 semiannual report;

- UW-Madison executed a $2.4 million contract for the Student Information System Upgrade in May 2019 but first reported this project to the Board of Regents in the September 2019 semiannual report; and

- UW System Administration executed two contracts totaling $745,000 for the Interactive Reporting Tool Replacement in November 2015 but first reported this project to the Board of Regents in the March 2016 strategic plan and semiannual report.

UW institutions, including UW System Administration, should comply with statutes by implementing only those IT projects approved by the Board of Regents. Doing otherwise undermines the statutorily prescribed oversight of the Board of Regents. If the Board of Regents withheld approval of a project for which a UW institution had already executed a contract, significant funds may be unnecessarily spent. Avoiding unnecessary expenditures will be even more important

in the coming years as UW System finances are affected by the COVID-19 pandemic.

☑ **Recommendation**

We recommend the University of Wisconsin System Administration:

- *ensure that University of Wisconsin institutions, including itself, comply with statutes by implementing only those information technology projects approved by the Board of Regents; and*

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

Procurement

We found a number of concerns with the procurement processes for the 10 projects we reviewed. UW institutions did not consistently:

- provide us with certain project-related contracts that we repeatedly requested;

- comply with Board of Regents policies by submitting certain information about large, high-risk IT projects to UW System Administration;

- review the terms of contracts negotiated by consortia before purchasing services through these contracts;

- comply with statutes by reporting quarterly to the Board of Regents on the expenditures of projects with open-ended contracts;

- comply with statutes by including 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;

- have contracts with firms that provide ongoing project work; and

- contractually specify monetary penalties for not completing work on time or within budget.

Locate Contracts

UW System Administration did not provide us with two master contracts that we repeatedly requested.

We requested all contracts associated with the 10 projects and found that UW institutions procured goods and services for 5 projects, in part, by using two master contracts that UW System Administration and UW-Madison had executed. UW institutions executed agreements that stipulated the terms and conditions of the project work to be provided, and the terms of the master contracts also applied. UW System Administration did not provide us with these two master contracts, even though we requested them each month from January 2020 through April 2020. As a result, we were unable to fully assess contractual obligations pertaining to these five projects, and UW System Administration was unable to demonstrate that it used the master contracts to manage ongoing relationships with the relevant firms that provided the project work.

UW Administration should ensure that it can readily locate all contracts for IT projects. Doing so will enable active management of the firms that provide the project work.

☑ Recommendation

We recommend the University of Wisconsin System Administration:

- *ensure that it can readily locate all contracts for information technology projects; and*

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

Submit Information

Board of Regents policies require UW institutions to submit to UW System Administration information about large, high-risk IT projects, including a project's governance structure, objectives, timeline, and budget. We found that UW System Administration did not require UW institutions to submit such information about large, high-risk IT projects. UW System Administration indicated that it interacts frequently with UW institutions and is familiar with such projects, and that it expects UW institutions to have such information available if it requests to review it.

UW System Administration should comply with Board of Regents policies by requiring UW institutions to submit to it certain information about their large, high-risk IT projects. If UW System Administration believes these policies are no longer necessary, it can work with the Board of Regents to modify them.

☑ Recommendation

We recommend the University of Wisconsin System Administration:

- *comply with Board of Regents policies by requiring University of Wisconsin institutions to submit to it certain information about their large, high-risk information technology projects; and*

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

Review Contracts

UW System Administration indicated that it generally followed DOA's IT procurement policies before December 2019. A DOA policy developed in September 2017 indicates that state agencies wishing to purchase goods and services through contracts negotiated by other state or federal agencies should first review these contracts and determine whether the contractual terms are acceptable.

UW-Madison did not review the terms of a consortium's contract through which it purchased services.

In November 2017, UW-Madison executed a one-year, automatically renewable contract with a consortium of higher education institutions that are located throughout the nation and work together to procure IT goods and services. This contract, which was for the Canvas Transition project, provided UW-Madison with access to a digital learning system that a firm had contractually provided to the consortium. UW-Madison indicated that because the consortium had a confidentiality agreement with the firm, it was unable to review the firm's contract with the consortium. When UW institutions do not review contracts, they could be unknowingly and adversely affected by the contractual terms.

In December 2019, UW System Administration implemented policies for procuring goods and services through contracts that consortia executed with other entities. To help ensure fair and open competition, these policies require UW institutions to review the terms and conditions of consortia contracts before procuring goods and services through those contracts.

UW System Administration should ensure that UW institutions comply with its December 2019 policy. It can do so, in part, by advising UW institutions to request its assistance if firms decline to reveal their contracts with consortia, thereby preventing UW institutions from understanding how they could be adversely affected by those contracts. Doing so will help to ensure that contractual provisions are known.

☑ **Recommendation**

We recommend the University of Wisconsin System Administration:

- *ensure that University of Wisconsin institutions comply with its policies relating to procuring goods and services through contracts with consortia, including by advising them to request its assistance if firms decline to reveal their contracts with consortia; and*

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

Report Quarterly

Statutes allow UW System to execute open-ended contracts for IT projects. Statutes define open-ended contracts as those that stipulate firms will deliver products or services but do not specify a maximum payment amount, those that stipulate firms will be paid an hourly wage but do not limit the number of hours required to complete projects, or both. Statutes require UW institutions to report to the Board of Regents each quarter on the expenditures of projects with open-ended contracts. UW System Administration informed us that it does not execute open-ended contracts and was unaware of any UW institution having executed them since FY 2013-14.

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.

However, we found that UW System Administration executed three open-ended contracts from FY 2013-14 through FY 2019-20. For example, UW System Administration executed an open-ended contract for the Student Information System Restructuring in October 2018. This contract stipulated the hourly rates to pay four consultants but did not limit the number of hours to complete the work. Although UW System Administration indicated that it considered a contract to be open-ended only if a UW institution had no way to terminate it, this is not the statutory definition of an open-ended contract.

UW System Administration should ensure that UW institutions, including itself, comply with statutes by reporting quarterly to the Board of Regents on the expenditures of projects with open-ended contracts. In doing so, UW System Administration should use the statutory definition of open-ended contracts. Doing so will facilitate the statutorily prescribed oversight required of the Board of Regents.

☑ **Recommendation**

We recommend the University of Wisconsin System Administration:

- *ensure that University of Wisconsin institutions, including itself, comply with statutes by reporting quarterly to the Board of Regents on the expenditures of information technology projects with open-ended contracts; and*

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

Include Contractual Stipulation

Statutes require the Board of Regents to include 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. Statutes allow the Board of Regents to exclude such a stipulation if it would negatively affect contract negotiations or the number of potential bidders, the contract includes alternate provisions to ensure it is completed on time and on budget, and the Board of Regents submits the alternative contractual provisions to the Joint Committee on Information Policy and Technology for approval.

None of the contracts we reviewed contained the statutorily required stipulation that the Board of Regents must approve certain orders or amendments.

None of the contracts we reviewed that were associated with the 9 projects contained the statutorily required stipulation that the Board of Regents must approve an order or amendment that would change the contract scope and increase the contract price. UW System Administration indicated that UW institutions, including itself, decide whether to approve such orders and amendments.

UW System Administration should ensure that UW institutions, including itself, comply with statutes by including 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. Doing so will facilitate the statutorily prescribed oversight required of the Board of Regents.

☑ **Recommendation**

We recommend the University of Wisconsin System Administration:

- *ensure that University of Wisconsin institutions, including itself, comply with statutes by including in contracts for large, high-risk information technology 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; and*

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

Have Contracts

UW-Madison did not have a contract with a firm over at least a six-month period when a project was ongoing.

We found that UW-Madison did not have a contract over at least a six-month period with a firm that provided ongoing work for the Canvas Transition. UW-Madison had a $16,000 contract with the firm from January 2018 until August 2018, and it paid the firm $16,600 in November 2018. UW-Madison reported to the Board of Regents in February 2019 that the firm had missed key deadlines for this project, which it reported was ongoing. UW-Madison could not explain to us why it did not have a contract with the firm after August 2018. UW-Madison executed a new $90,000, annually renewable contract with the firm in May 2019.

UW institutions should have contracts with firms that provide it with ongoing project work. Without contracts, UW institutions cannot hold firms legally responsible for completing work in a timely manner, to the necessary standards, and for the agreed-upon amounts.

☑ **Recommendation**

We recommend the University of Wisconsin System Administration:

- *ensure that University of Wisconsin institutions have contracts with firms that provide ongoing work for information technology projects; and*

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

Specify Penalties in Contracts

A UW-Stevens Point contract did not require a firm to pay monetary penalties for not completing work on-time for a large, high-risk IT project.

In April 2015, UW-Stevens Point executed a $3.2 million contract with a firm to provide project management and other consulting services for the Student Information System Implementation, which was a large, high-risk IT project. We found that this contract did not require the firm to pay monetary penalties for not completing work on time or within the contractually established budget. This project was completed nine months after the original expected completion date and cost $1.0 million more than originally anticipated. UW-Stevens Point indicated that this occurred, in part, because the firm did not complete contractually specified work on time and on budget.

UW System Administration should require UW institutions to contractually specify monetary penalties for not completing project work on time and on budget. Doing so will help to ensure that projects are completed on time and on budget.

☑ Recommendation

We recommend the University of Wisconsin System Administration:

- *require University of Wisconsin institutions to contractually specify monetary penalties for not completing information technology project work on time and on budget; and*

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

Project Reporting

As noted, by each March 1 and September 1, statutes require the Board of Regents to submit to the Joint Committee on Information Policy and Technology a semiannual report on large, high-risk IT projects. Statutes require these reports to contain certain information, including:

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

- any contract executed by the Board of Regents for a project;

- 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.

The semiannual reports did not include information about all large, high-risk IT projects, or accurate and complete information about the projects that were included.

We reviewed the semiannual reports that the Board of Regents submitted to the Joint Committee on Information Policy and Technology from March 2014 through March 2020. We found that these reports did not include information about all large, high-risk IT projects. In addition, these reports did not include accurate and complete information about the projects that were included.

The semiannual reports we reviewed did not include all projects managed by UW System Administration. We found that UW System Administration executed:

- a $1.1 million contract with a firm to help plan an HRS upgrade in January 2014 but did not include this planning project in any semiannual report from March 2014 through March 2020; and
- a $1.5 million contract with a firm to help plan the Budgeting, Planning, and Forecasting System in August 2015 but did not include this planning project in any semiannual report from September 2015 through March 2020.

UW System Administration did not consistently include accurate information about the budgets of its projects in the semiannual reports we reviewed. UW System Administration indicated:

- in the September 2016 through March 2018 semiannual reports that the HRS Upgrade budget was $7.5 million, but documents it provided to us indicated that the budget increased to $8.4 million in April 2017 because the project's scope expanded;
- in the September 2017 through March 2019 semiannual reports that the Shared Financial System Upgrade budget was $7.9 million, but documents it provided to us indicated that the budget was $8.4 million because another project was combined with the Upgrade project; and

- in the March 2019 through March 2020 semiannual reports that the Student Success Collaborative budget was $10.7 million, but documents it provided to us indicated that the project's budget was $11.2 million, including the costs of project administration.

The March 2020 semiannual report included 17 projects for which anticipated costs were listed. Nine 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 two projects were each anticipated to cost more than $10.0 million. We found that this report included statutorily required information on project funding sources for only 1 of all 19 projects listed. UW System Administration informed the Board of Regents that it had summarized the information it had received from UW institutions in order to reduce the burden on the Board of Regents.

UW System Administration should ensure that the semiannual reports submitted to the Joint Committee on Information Policy and Technology consistently contain all statutorily required information for all large, high-risk IT projects. Doing so will facilitate legislative oversight of these projects.

☑ Recommendation

We recommend the University of Wisconsin System Administration:

- *ensure that the semiannual reports submitted to the Joint Committee on Information Policy and Technology consistently contain all statutorily required information for all large, high-risk information technology projects; and*

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

■ ■ ■ ■

Cloud Computing ■

We evaluated UW System's management of IT projects involving cloud computing services provided by firms.

We evaluated UW System's management of IT projects involving cloud computing services provided by firms. To do so, we analyzed six projects involving cloud computing services provided by firms and a seventh project that preplanned a cloud computing project. The seven projects were managed by one or more of the following UW institutions: UW System Administration, UW-Eau Claire, UW-Madison, UW-Milwaukee, and UW-Stevens Point. We found that these UW institutions 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 also found that UW System Administration did not consistently obtain the necessary approval from the Board of Regents before implementing large, high-risk IT projects or provide the Board of Regents with all statutorily required information about such projects. We provide recommendations for improvements.

Policies

We found that UW System Administration established few policies that specifically address how UW institutions are to acquire cloud computing services from firms. Instead, it indicated that it relied on its general IT policies. In December 2019, UW System Administration provided us with draft policies for assessing the IT security of firms that provide IT services, including cloud computing services. These draft policies, which had not been implemented as of May 2020, would

require UW System Administration to complete formal risk assessments before granting firms access to UW System's data and IT systems.

We found concerns with UW System Administration's draft policies for assessing the IT security of firms that provide IT services, including cloud computing services.

We found concerns with UW System Administration's draft policies for assessing the IT security of firms that provide IT services, including cloud computing services. First, these draft policies specify how UW System Administration is to assess IT security at these firms, but they do not require UW institutions to take the assessment results into consideration when determining whether to contract with them. Second, these draft policies do not require UW institutions to periodically assess the IT security of firms that contractually provide them with cloud computing services, such as by obtaining and reviewing annual IT security audits of the firms.

UW System Administration should implement policies for assessing the IT security of firms that provide cloud computing services. The policies should require UW institutions to take the results of IT security assessments into consideration before contracting with firms. The policies should also require UW institutions to annually assess the IT security of firms that contractually provide cloud computing services, such as by obtaining and reviewing IT security audits of the firms. Doing so will help to ensure the security of UW System's data and IT systems.

☑ Recommendation

We recommend the University of Wisconsin System Administration:

- *implement policies that require University of Wisconsin institutions to take into consideration the results of information technology security assessments before contracting with firms that provide cloud computing services, and to annually assess the information technology security at such firms; and*

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

In response to our January 2020 survey, every UW institution indicated that it used cloud computing services provided by firms. Nine UW institutions indicated that they had policies and procedures governing the procurement and management of cloud computing services provided by firms, but four UW institutions indicated that they did not have them or were uncertain whether they had them. Most of the nine UW institutions 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 contractual terms regarding data security;
- required standard contractual terms ensuring that UW System retains ownership of data stored by such firms; and
- required security or risk assessments before using services provided by such firms.

The cloud computing policies of UW institutions were incomplete.

The cloud computing policies of UW institutions were incomplete. Less than one-half of the nine UW institutions indicated that their policies and procedures required them to evaluate whether to use the services provided by UW System Administration before seeking cloud computing services provided by firms. Similarly, less than one-half indicated that their policies and procedures specified requirements for successfully managing a migration to using cloud computing services provided by firms.

UW System Administration should ensure that all UW institutions have complete policies for using cloud computing services provided by firms. Such policies should require UW institutions to evaluate whether to use the services provided by UW System Administration before using cloud computing services provided by firms, and they should specify requirements for successfully managing a migration to using cloud computing services provided by firms.

☑ Recommendation

We recommend the University of Wisconsin System Administration:

- *ensure that all University of Wisconsin institutions have complete policies for using cloud computing services provided by firms; and*
- *report to the Joint Legislative Audit Committee by January 15, 2021, on its efforts to implement this recommendation.*

Projects

We reviewed six projects involving firms that provided cloud computing services and a seventh project that preplanned a cloud computing project. The seven projects we reviewed began from FY 2010-11 through FY 2019-20 and include:

- UW System Administration's and UW-Madison's Preplanning for the Administrative Transformation Program, which is expected to replace UW System's human resource system and financial system;
- UW-Milwaukee's Microsoft Teams, which enables telephone and teleconferencing over the internet;
- UW-Stevens Point's Ellucian, which helps to communicate with prospective students;
- UW-Eau Claire's Maxient, which helps to manage student behavioral records;
- UW System Administration's Budgeting, Planning, and Forecasting System, which is expected to help analyze expenditures and revenues, plan budgets, and help strategic planning and analysis;
- UW-Madison's Facilities Planning and Management Work Order System, which is expected to help manage facilities maintenance, campus renovation projects, and capital planning and development; and
- UW-Madison's Database Environment Refresh, which is expected to replace the hardware and database environment for accounting, payroll, benefits, and student information applications.

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

As shown in Table 5, three of the seven projects were completed, and the other four projects were ongoing at the time of our fieldwork. The projects administered by UW-Milwaukee, UW-Eau Claire, and UW-Stevens Point were not reported as large, high-risk IT projects, but the other four were reported as large, high-risk IT projects.

Table 5

UW System Cloud Computing Projects Reviewed

		Information That UW Institutions Reported to the Board of Regents		
	UW Institution	Start Date	Completion Date	Expenditures
Completed Projects[1]			**Actual**	
Microsoft Teams	Milwaukee	Sept. 2018	April 2020	$ 1,231,200
Ellucian	Stevens Point	June 2018	Sept. 2018	62,000
Maxient	Eau Claire	May 2011	April 2012	18,300
Ongoing Projects			**Estimated**	
Preplanning for the Administrative Transformation Program Project	System Administration, Madison	Jan. 2019	–[2]	10,618,900
Budgeting, Planning, and Forecasting System	System Administration	July 2016	Dec. 2021	8,150,000
Facilities Planning and Management Work Order System	Madison	Aug. 2018	Jan. 2021	4,655,000
Database Environment Refresh	Madison	April 2019	July 2020	1,114,000

[1] These projects were not reported to the Board of Regents as large, high-risk IT projects.

[2] In June 2020, UW System Administration was uncertain when this project will be completed.

We assessed the extent to which UW institutions incorporated into these seven 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 UW System's data.

Needs Assessment and Procurement

The federal General Services Administration recommends evaluating the advantages and disadvantages of transitioning to cloud computing services provided by firms. We reviewed relevant documentation that UW institutions provided for six of the seven projects, but we did not do so for Maxient because UW-Eau Claire completed needs assessment tasks for this project a number of years ago.

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

We found that UW institutions did not consistently evaluate in writing the advantages and disadvantages of transitioning to cloud computing services provided by firms. They conducted such evaluations for the Database Environment Refresh and the Facilities Planning and Management Work Order System, but they did not do so for four other projects we reviewed.

In some instances, UW institutions may possess insufficient knowledge to successfully evaluate a transition to cloud computing services. UW-Milwaukee spent at least $195,400 to begin a project that did not rely on such services, but the firm providing the project's software subsequently advised UW-Milwaukee to purchase the cloud computing-based software to which the firm was transitioning. UW-Milwaukee indicated it had been unaware of how quickly the firm was transitioning to the cloud computing-based software.

UW System Administration should ensure that UW institutions, including itself, consistently evaluate in writing the advantages and disadvantages of transitioning to cloud computing services provided by firms before beginning projects that make such a transition. Doing so is important because such firms may store confidential data, including personal data pertaining to UW System employees and students. In addition, if a UW institution determines that it should not have made such a transition, it could be challenging, time-consuming, and expensive to complete a second project.

☑ Recommendation

We recommend the University of Wisconsin System Administration:

- *ensure that University of Wisconsin institutions, including itself, consistently evaluate in writing the advantages and disadvantages of transitioning to cloud computing services provided by firms before beginning projects that make such a transition; and*

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

Data Security

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

We found that UW institutions 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 UW institutions provided us for the projects we reviewed. We did not complete all such work for certain projects. For example, we did not do so for the Preplanning for the Administrative Transformation Program because the Preplanning project did not involve firms that provided cloud computing services.

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 UW institutions:

- contractually required a firm for one project to submit annual IT security audits but did not document its reviews of these audits; and

- did not contractually require firms for four projects to submit annual IT security audits.

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

- contractually required a firm for one project to store UW System's data in the U.S.; and

- did not contractually require firms for four projects to do so.

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 UW institutions:

- contractually required a firm for one project to conduct criminal background checks; and

- did not contractually require firms for four projects 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 UW institutions:

- contractually required firms for two projects to limit employee access to their data; and
- did not contractually require firms for three projects to do so.

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 UW institutions:

- contractually required firms for two projects to pay monetary penalties and assume such responsibility; and
- did not contractually require firms for three projects to do so.

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 UW institutions:

- contractually required firms for four projects to notify them of security breaches and unauthorized data disclosures; and
- did not contractually require the firm for one project to do so.

UW System Administration noted the importance of assessing the IT security of firms that provide cloud computing services because UW System does not maintain full control over data stored by these firms. It should require UW institutions, including itself, that contract with firms that provide cloud computing services to take appropriate actions to safeguard UW System'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 UW System'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 UW System's data;

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

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

☑ Recommendation

We recommend the University of Wisconsin System Administration:

- *require University of Wisconsin institutions, including itself, that contract with firms to provide cloud computing policies to take various appropriate actions to safeguard the University of Wisconsin System's data; and*

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

Preplanning for the Administrative Transformation Program

In February 2019, UW System Administration informed the Board of Regents that it had begun a Preplanning project for the Administrative Transformation Program.

In February 2019, UW System Administration informed the Board of Regents that it and UW-Madison had begun a preplanning project associated with a cloud computing-based enterprise resource IT system known as the Administrative Transformation Program. This new system is intended to replace UW System's current payroll system, HRS, and its current financial system, Shared Financial System. UW System Administration indicated that these payroll and financial systems no longer meet its needs and those of UW-Madison, and that it plans to implement the new system at all UW institutions. As we noted in report 14-4, UW System spent $78.6 million to plan and implement HRS, with consulting services

accounting for almost two-thirds of this amount. HRS was largely implemented in April 2011, and an upgrade was completed in 2017.

UW-Madison provided us with summary information indicating that UW System annually spends from $11.4 million to $21.1 million on IT systems that help to ensure enterprise systems, including HRS, meet its needs. This information, which a consultant compiled, did not explain in detail how these amounts were calculated. UW-Madison indicated that the Administrative Transformation Program will use current cloud computing technology to redesign and increase the efficiency of various operational processes.

We found concerns with how UW System Administration administered the Preplanning project, which is estimated to cost $10.6 million.

We found concerns with how UW System Administration administered the Preplanning project, which is estimated to cost $10.6 million. UW System Administration:

- began the Preplanning project before obtaining approval from the Board of Regents to do so;
- executed a $2.3 million contract without obtaining approval from the Board of Regents; and
- did not provide all statutorily required information about the project to the Board of Regents.

Although statutes allow UW institutions to implement only those IT projects approved by the Board of Regents, UW System Administration informed the Board of Regents in February 2019 that it had already begun the Preplanning project. UW System Administration listed the project in the March 2019 semiannual report on large, high-risk IT projects, and the Board of Regents approved this report. UW System Administration did not provide the Board of Regents with a project cost estimate in February 2019.

Board of Regents policies require the Board of Regents to approve some, but not all, contracts of more than $1.0 million with firms. In April 2019, UW System Administration executed a $2.3 million contract with a consultant to provide services for the Preplanning project. UW System Administration chose to execute this contract under policy provisions that did not require it to obtain approval from the Board of Regents.

In July 2019, UW System Administration informed the Board of Regents that the Preplanning project's budget was $3.2 million, including consultant costs. UW System Administration noted that UW System staff costs were excluded from this amount.

In February 2020, UW System Administration informed the Board of Regents that the Preplanning project's budget had increased to $10.6 million. This amount included $4.3 million for UW System staff costs. It also indicated that consultant costs had increased to $4.9 million but did not explain why this increase had occurred. The Board of Regents approved a UW System Administration request to lease 18,900 square feet of office space for five years for 150 individuals to work on the Administrative Transformation Program, which the Board of Regents had not yet approved. The five-year rent will total $2.7 million, and UW System Administration intends to make $600,000 in improvements to this office space.

Although statutes require the semiannual reports that the Board of Regents submits to the Joint Committee on Information Policy and Technology to include the original and updated costs of each large, high-risk IT project, as well as explanations for any variation between these costs, we found that the March 2019 and September 2019 reports excluded UW System staffing costs for the Preplanning project. The March 2020 report included these costs, but none of the three reports fully explained why project costs had increased over time.

In August 2020, UW System Administration informed the Board of Regents that it expected to request approval from the Board of Regents in October 2020 to initiate the Administrative Transformation Program, and that it expected to begin this project in January 2021. However, by the time the Board of Regents is asked to approve this project, UW System Administration will have committed to spending at least $10.6 million on the Preplanning project and leasing office space for 150 individuals.

■ ■ ■ ■

IT Security ■

Managing cybersecurity risk is critical to ensuring UW System's overall IT security.

Managing cybersecurity risk is critical to ensuring UW System's overall IT security. Board of Regents policies require UW System Administration to develop and maintain a comprehensive information security program that addresses issues such as system access and authentication; system and data integrity; data access, privacy, and confidentiality; and incident response. These policies also require each UW institution to consistently apply this information security program and monitor compliance with it. UW System Administration is responsible for establishing systemwide policies. We reviewed IT security at five UW institutions and found a number of concerns. We recommend UW System Administration take steps to improve IT security and report on its progress in addressing these concerns.

We found IT security concerns in our prior audits of UW System. We reported concerns in our financial audits of UW System for FY 2014-15 (report 16-3), FY 2015-16 (report 17-6), and FY 2016-17 (report 18-2). In our *State of Wisconsin FY 2017-18 Single Audit* (report 19-3), we again reported these concerns and noted that UW System Administration had not made significant progress in developing systemwide policies. As part of our FY 2018-19 Single Audit (report 20-3), we followed up on these concerns and found that UW System Administration had partially implemented recommendations we made. Future audits will follow up on these issues.

IT Security Concerns

UW System retains a variety of data to administer its programs, including confidential and sensitive data such as personally identifiable information and student educational records. To protect these data and ensure the continuity of operations, it is important for UW System to maintain appropriate IT security measures. These measures should form layers of defense that, when working together, protect UW System'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, UW System Administration 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 an entity such as UW System 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.

UW System Administration did not develop comprehensive IT security policies and procedures.

We found that UW System Administration did not develop comprehensive IT security policies and procedures for it and all other UW institutions. At the time of our fieldwork, UW System Administration had developed 5 policies, each of which it had issued

in 2016 or earlier, and was in the process of developing 11 additional policies. Although it expected to complete some of these 11 policies in summer 2020, it did not provide us with a timeline for completing all of them. At the time of our fieldwork, these 11 policies were in various stages of development, and it was unclear whether they would form a comprehensive set of policies when completed. UW System Administration indicated that it may develop procedures pertaining to these policies. We also found that the extent of policies and procedures developed by individual UW institutions varied, and that UW institutions awaited completion of UW System Administration's policies. Incomplete policies and procedures increase the risk that UW System's data and systems may not be adequately protected.

Our review of IT security at five UW institutions found 46 concerns pertaining to the five core functions of the NIST cybersecurity framework.

Our high-level review of IT security at five UW institutions found 46 concerns pertaining to the five core functions of the NIST cybersecurity framework. We found concerns at all five of the UW institutions we reviewed. 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 UW System Administration.

UW System Administration should develop comprehensive IT security policies and procedures that are based on the NIST standards. UW System Administration should address each of the 46 IT security concerns that we found, and it should ensure all UW institutions, including itself, comply with its policies and procedures. To help ensure this occurs, UW System Administration 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 UW System. We plan to conduct future audit work to ascertain IT security throughout UW System, including the extent to which UW System Administration has implemented our recommendations.

☑ Recommendation

We recommend the University of Wisconsin System Administration;

- *develop comprehensive information technology security policies and procedures that are based on National Institute of Standards and Technology standards;*

- *address each of the 46 information technology security concerns that we found;*

- *ensure all University of Wisconsin institutions, including itself, comply with its policies and procedures; and*

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

■■■■

Improving Oversight ■

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. Board of Regents policies do not require UW institutions to request Board of Regents approval to execute all IT contracts of more than $1.0 million, and UW institutions did not consistently comply with statutory and other requirements pertaining to their management of projects. To improve oversight, we recommend that UW System Administration work with the Board of Regents to modify policies and establish an IT projects committee of the Board of Regents to provide additional oversight of projects, including large, high-risk IT projects.

Board of Regents Policies

We found that UW institutions executed IT contracts under the authority of multiple statutory chapters, including:

- ch. 16, Wis. Stats., which delegated to the Board of Regents the authority to make purchases under DOA's general procurement authority; and

- ch. 36, Wis. Stats., which authorizes the Board of Regents to purchase materials, supplies, equipment, or services that relate to higher education and that state agencies other than UW System do not commonly purchase.

Approval by the Board of Regents of a given IT contract depends, in part, on the particular statutory authority UW institutions choose to use when executing a contract.

Approval by the Board of Regents of a given IT contract depends, in part, on the particular statutory authority that UW institutions choose to use when executing a contract. As shown in Table 6, Board of Regents policies do not require UW institutions to obtain approval from the Board of Regents before executing contracts under the authority of ch. 16, Wis. Stats., regardless of the amount of the contracts. DOA also does not approve such contracts because statutes delegated purchasing authority to the Board of Regents. In contrast, policies require UW institutions to obtain approval from the Board of Regents before executing contracts under the authority of ch. 36, Wis. Stats., and that are more than $1.0 million. UW System Administration indicated that it determines whether to make purchases under the authority of ch. 36, Wis. Stats., based on discussions among its staff, rather than on written policies. It indicated that approximately 80.0 percent of all UW System purchases are made under the authority of ch. 16, Wis. Stats., and are not approved by the Board of Regents.

Table 6

Board of Regents Approval Needed to Execute IT Contracts

Statutes	Types of Contracts	Board of Regents Approval Required[1]
Chapter 16	Goods and services that state agencies commonly purchase	None
Chapter 36	Materials, supplies, equipment, or services that relate to higher education and that state agencies other than UW System do not commonly purchase	Contracts of more than $1.0 million

[1] As required by Board of Regents policies.

The Board of Regents did not approve IT contracts executed under the authority of ch. 16, Wis. Stats., and that were more than $1.0 million. For example:

- In April 2019, UW-Madison executed two contracts totaling $4.2 million with a firm for the Database Environment Refresh without obtaining approval from the Board of Regents.

- In April 2019, UW System Administration executed a $2.3 million contract for the Preplanning for the Administrative Transformation Program without obtaining

approval from the Board of Regents. UW System Administration indicated that it did not intend to seek approval to execute contracts for the Administrative Transformation Program, if the Board of Regents approves this project.

For the 17 projects we reviewed, UW institutions did not ask the Board of Regents to approve 12 contracts with a combined value of $27.8 million.

Approving all IT contracts of more than $1.0 million would not be burdensome for the Board of Regents. We assessed all of the contracts we were provided for the 17 projects we reviewed and found that UW institutions did not ask the Board of Regents to approve 12 contracts that were each more than $1.0 million. These 12 contracts, which UW institutions executed from April 2015 through December 2019, had a combined value of $27.8 million and were associated with 8 of the 17 projects.

UW System Administration should work with the Board of Regents to modify policies to require the Board of Regents to approve all IT contracts that are more than $1.0 million, regardless of the statutory authority under which they are executed. Doing so will help to ensure that the Board of Regents has consistent oversight of projects, particularly those that are large, high-risk IT projects.

☑ Recommendation

We recommend the University of Wisconsin System Administration:

- *work with the Board of Regents to modify policies to require the Board of Regents to approve all information technology contracts that are more than $1.0 million; and*

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

IT Projects Committee

UW System Administration should work with the Board of Regents to establish an IT projects committee to help it oversee projects, including large, high-risk IT projects.

UW System Administration should work with the Board of Regents to establish an IT projects committee of the Board of Regents to help oversee projects, including large, high-risk IT projects. Such a committee can work with UW System Administration to require UW institutions to obtain Board of Regents approval before executing all IT contracts that are more than $1.0 million. It can also review the annual IT strategic plans and provide appropriate guidance, including about whether UW System should initiate a given project. Doing so will be important in the coming years as UW System finances are affected by the COVID-19 pandemic.

An IT projects committee of the Board of Regents can help to ensure that UW institutions effectively, consistently, and appropriately manage projects.

An IT projects committee of the Board of Regents can help to ensure that UW institutions effectively, consistently, and appropriately manage projects. UW institutions, including UW System Administration, did not consistently comply with statutes, policies, and best practices for managing projects. As noted:

- 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.

- 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.

- UW System Administration and UW-Madison implemented projects before obtaining the statutorily required approval from the Board of Regents to do so.

- 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.

- UW-Madison did not review the terms of a consortium's contract through which it purchased services.

- UW System Administration did not comply with statutes because it did not report each quarter to the Board of Regents on the expenditures of projects with open-ended contracts.

- UW institutions did not comply with statutes because they did not 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.

- UW-Madison did not have a contract with a firm over at least a six-month period when a project was ongoing.

- UW-Stevens Point did not contractually require a firm to pay monetary penalties for not completing the work on time for a large, high-risk IT project.

- UW System Administration did not include information about all large, high-risk IT projects in the statutorily required 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.

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

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

- UW System Administration did not develop comprehensive IT security policies, and we found 46 concerns pertaining to IT security at five UW institutions.

☑ Recommendation

We recommend the University of Wisconsin System Administration:

- *work with the Board of Regents to establish an information technology projects committee; and*

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

■ ■ ■ ■

Appendix ■

Appendix

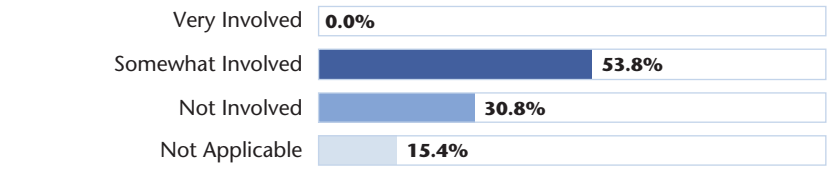
Opinions of UW Institutions

In January 2020, we surveyed every UW institution except for UW System Administration about various issues pertaining to IT needs assessment and procurement, cloud computing, and IT security. Each UW institution responded to our survey, but not all responded to each survey question.

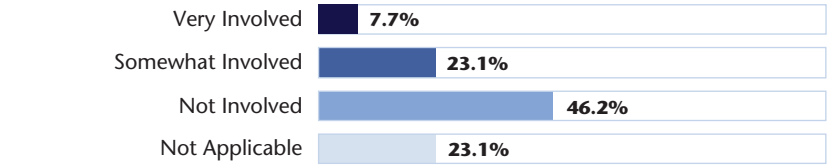
The following pages summarize the responses of UW institutions to our survey.

UW System Administration's Involvement with Selected IT Tasks at UW Institutions[1]

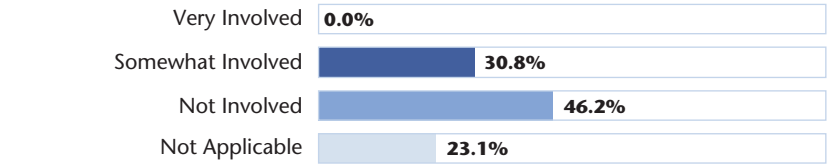
Assessing the Need for New or Improved IT Products



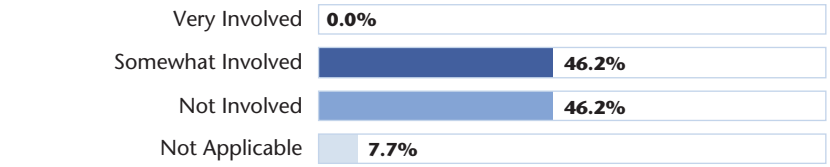
Conducting Cost-Benefit Analyses of Proposed IT Products



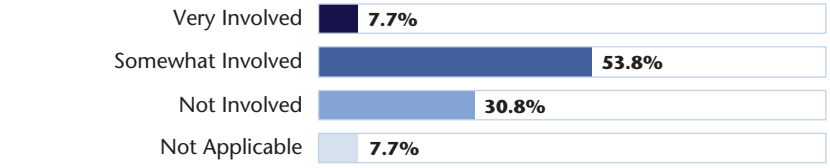
Assessing Commercially Available Off-the-Shelf IT Products



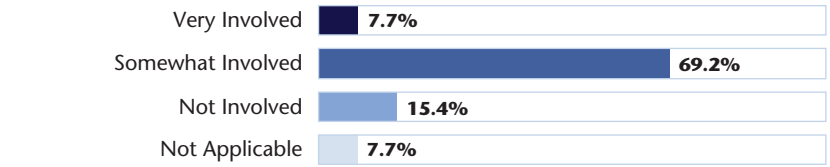
Assessing Whether IT Products or Contracts at Other Entities Could Meet a UW Institution's Needs



Developing Procurement Plans and Solicitations



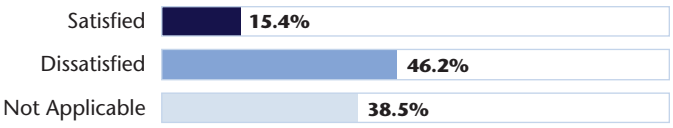
Developing or Negotiating Contracts with IT Vendors



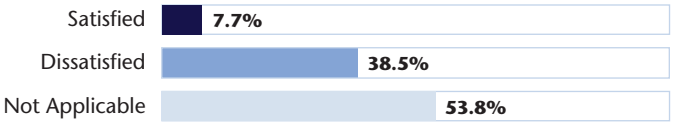
[1] According to survey respondents.

Satisfaction with UW System Administration's Involvement with Selected IT Tasks[1]

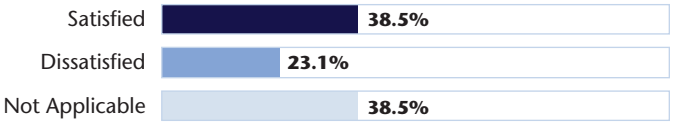
Assessing the Need for New or Improved IT Products



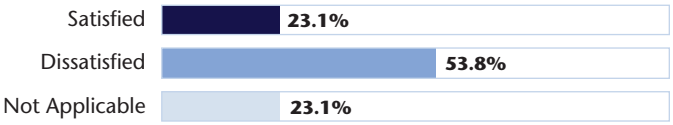
Conducting Cost-Benefit Analyses of Proposed IT Products



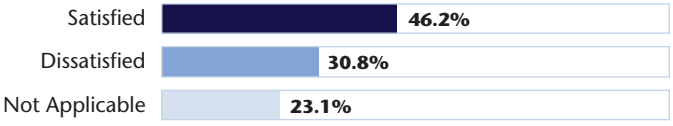
Assessing Commercially Available Off-the-Shelf IT Products



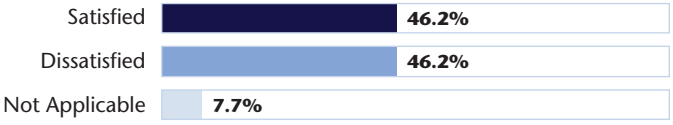
Assessing Whether IT Products or Contracts at Other Entities Could Meet a UW Institution's Needs



Developing Procurement Plans and Solicitations



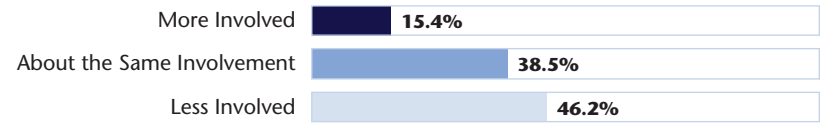
Developing or Negotiating Contracts with IT Vendors



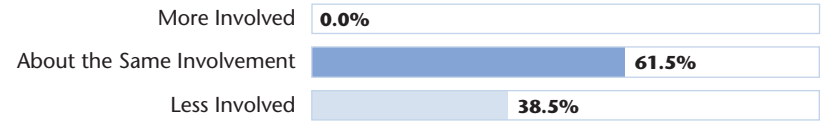
[1] According to survey respondents.

UW Institutions' Preferred Level of Involvement of UW System Administration with Selected IT Tasks[1]

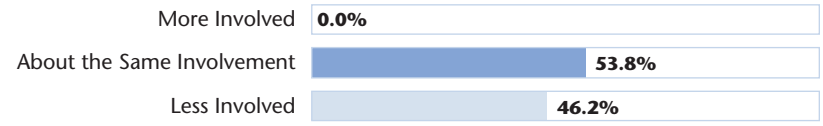
Assessing the Need for New or Improved IT Products



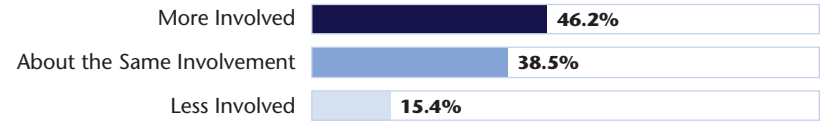
Conducting Cost-Benefit Analyses of Proposed IT Products



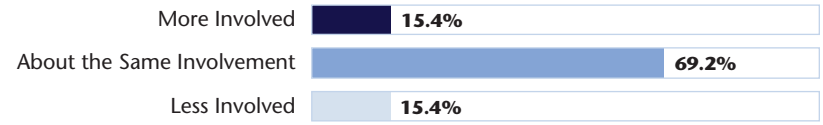
Assessing Commercially Available Off-the-Shelf IT Products



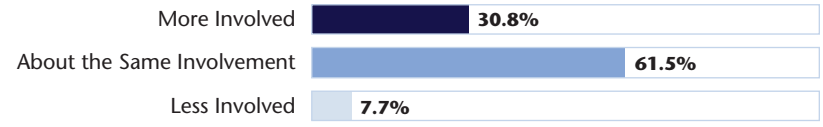
Assessing Whether IT Products or Contracts at Other Entities Could Meet a UW Institution's Needs



Developing Procurement Plans and Solicitations



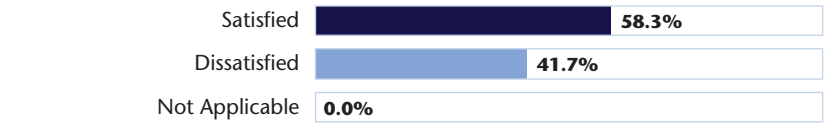
Developing or Negotiating Contracts with IT Vendors



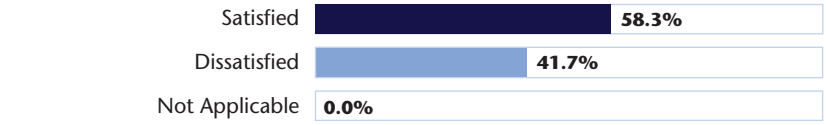
[1] As indicated by survey respondents.

Satisfaction of UW Institutions with the Enterprise IT Products Provided by UW System Administration[1]

Types of Products



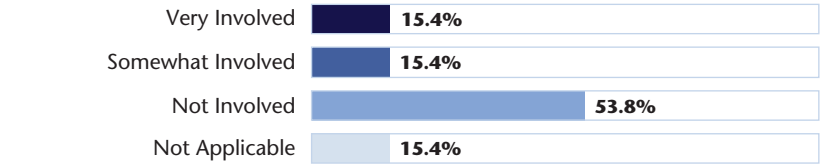
Quality of Products



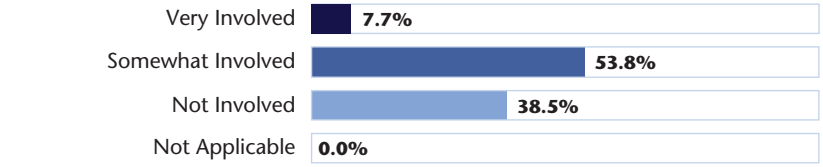
[1] As indicated by survey respondents.

UW System Administration's Involvement in Helping UW Institutions with Selected Cloud Computing Tasks[1]

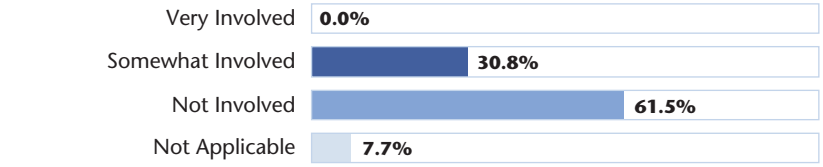
Identifying Services Provided by UW System Administration That Could Serve as Alternatives to Cloud Computing Services Provided by Firms



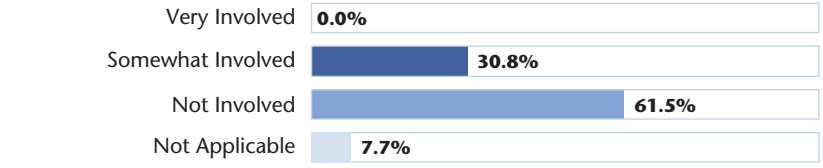
Developing Procurement Plans and Solicitations for Cloud Computing Services



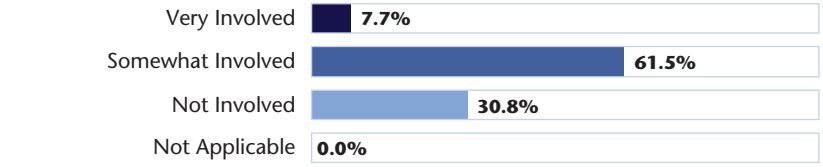
Evaluating the Quality of Cloud Computing Services Provided by Potential Vendors



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



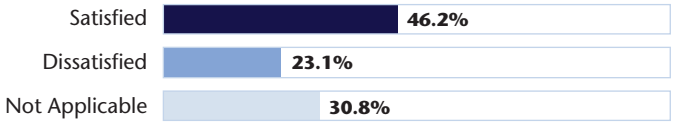
Developing and Negotiating Contracts with Firms That Provide Cloud Computing Services



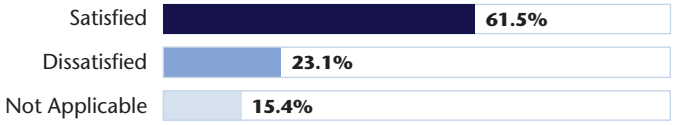
[1] As indicated by survey respondents.

Satisfaction of UW Institutions with UW System Administration's Involvement with Selected Cloud Computing Tasks[1]

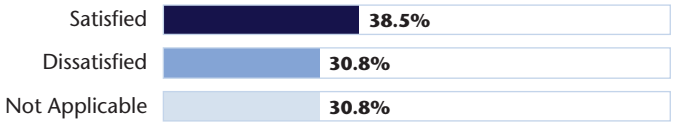
Identifying Services Provided by UW System Administration That Could Serve as Alternatives to Cloud Computing Services Provided by Firms



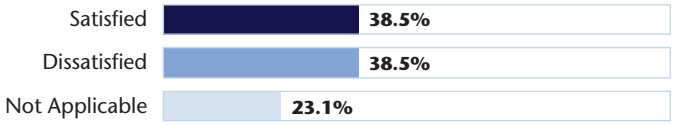
Developing Procurement Plans and Solicitations for Cloud Computing Services



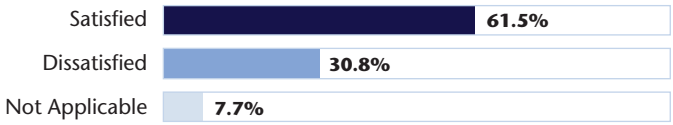
Evaluating the Quality of Cloud Computing Services Provided by Potential Vendors



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



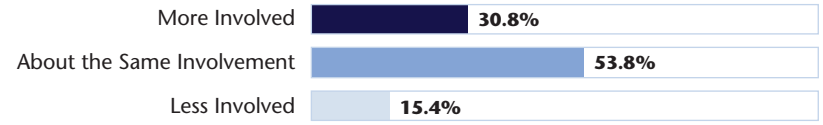
Developing and Negotiating Contracts with Firms That Provide Cloud Computing Services



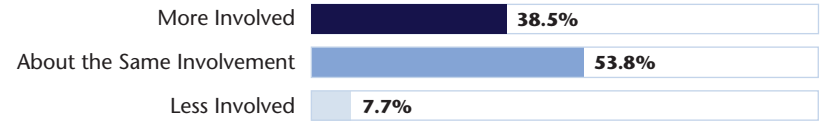
[1] As indicated by survey respondents

UW Institutions' Preferred Level of Involvement of UW System Administration with Selected Cloud Computing Tasks[1]

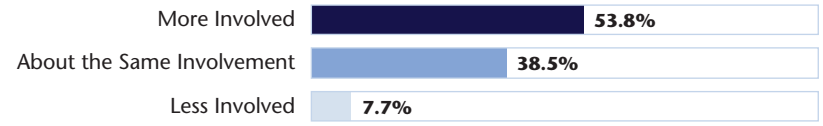
Identifying Services Provided by UW System Administration That Could Serve as Alternatives to Cloud Computing Services Provided by Firms



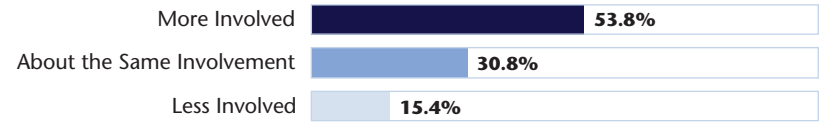
Developing Procurement Plans and Solicitations for Cloud Computing Services



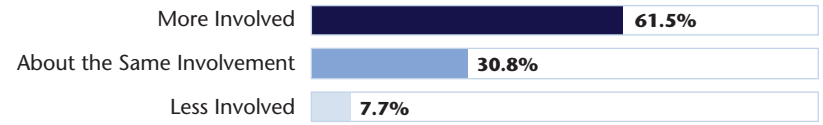
Evaluating the Quality of Cloud Computing Services Provided by Potential Vendors



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



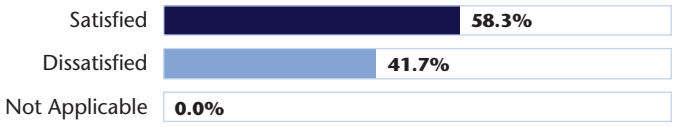
Developing and Negotiating Contracts with Firms That Provide Cloud Computing Services



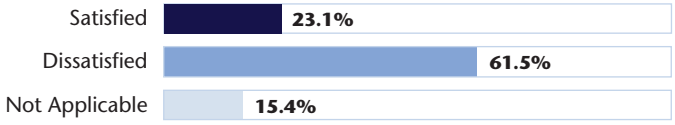
[1] As indicated by survey respondents.

Satisfaction of UW Institutions with Selected IT Security Services Provided by UW System Administration[1]

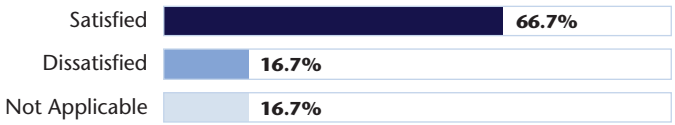
IT Security Policy Development



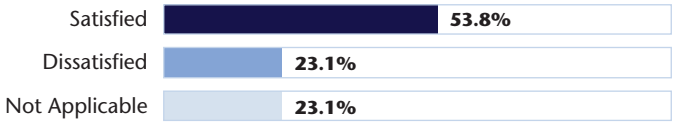
IT Security Policy Implementation



IT Security at DoIT's Data Center

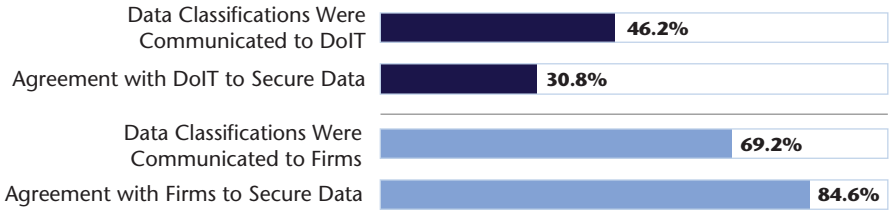


IT Security of Firms Managed by UW System Administration



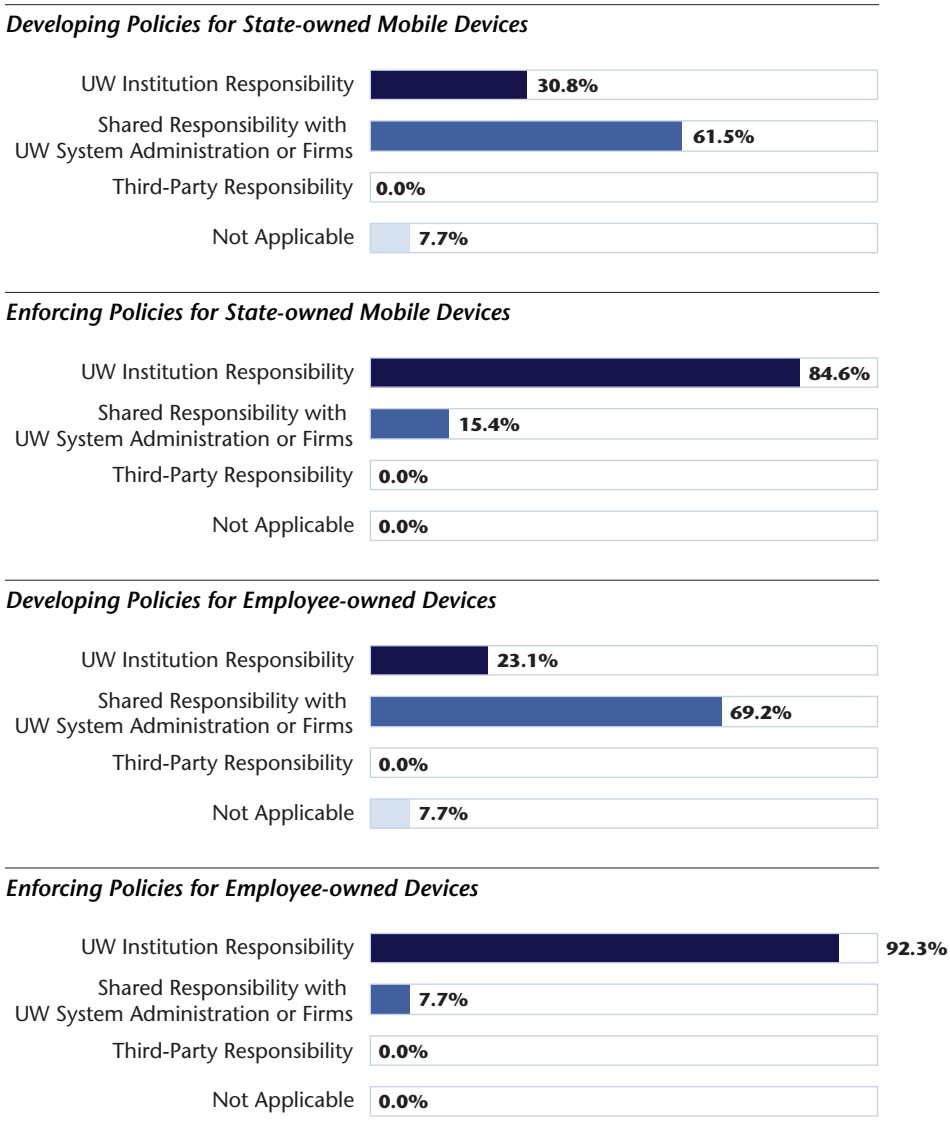
[1] As indicated by survey respondents.

Extent to which UW Institutions Communicated Their Data Classifications and Had Security Agreements[1]



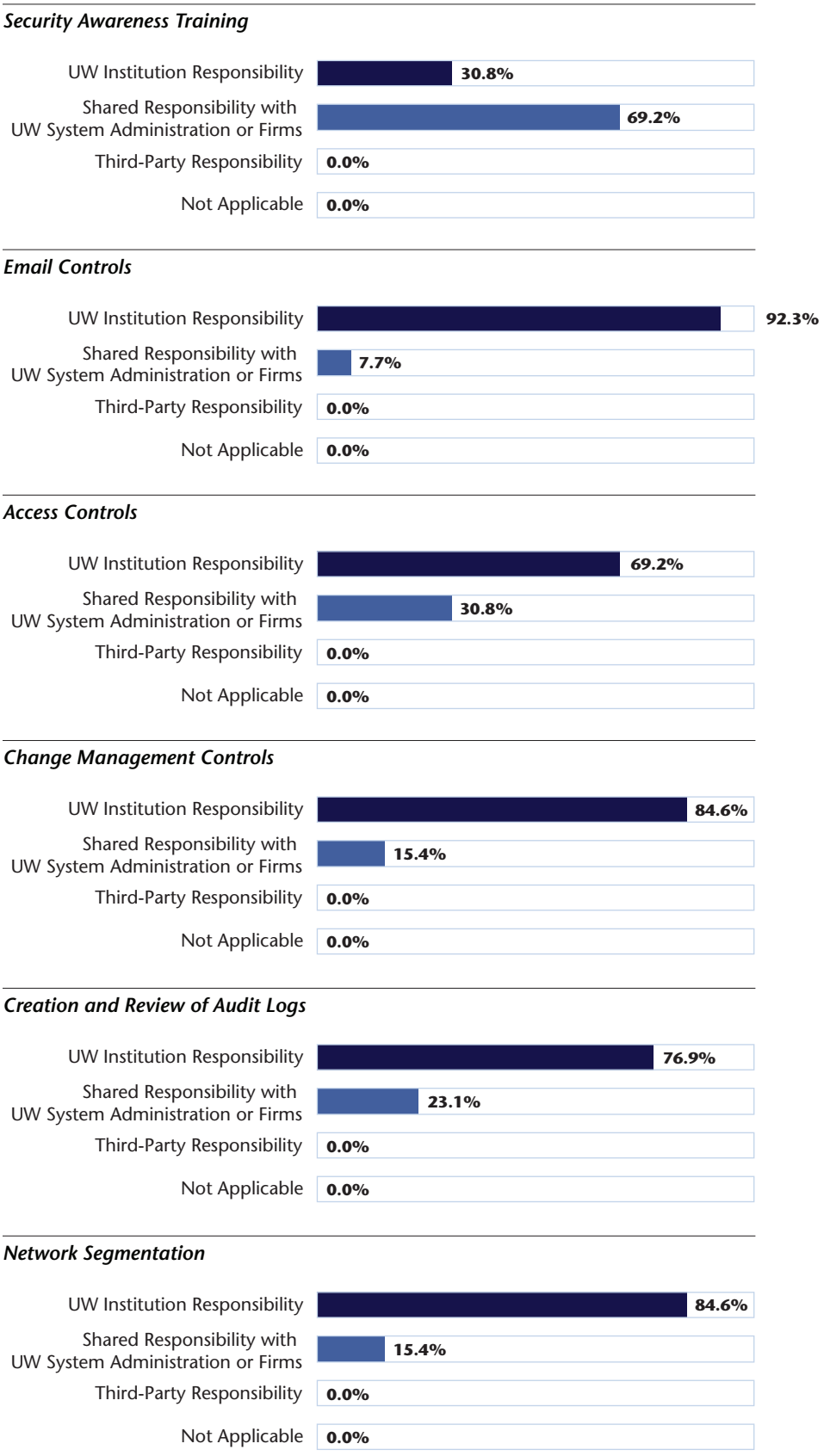
[1] As indicated by survey respondents. Percentages do not total to 100.0 percent because survey respondents could provide multiple answers.

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 ■

UNIVERSITY OF WISCONSIN SYSTEM

Office of the President
1700 Van Hise Hall
1220 Linden Drive
Madison, Wisconsin 53706-1559
608-262-2321
tthompson@uwsa.edu
www.wisconsin.edu

September 15, 2020

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

Dear State Auditor Chrisman,

Thank you for the opportunity to respond to the Legislative Audit Bureau's (LAB) review of the University of Wisconsin (UW) System's information technology (IT) security and IT needs assessment and procurement processes. Given the expansive nature of the audit, we continue to review the report and assess its findings.

I am committed to reviewing these recommendations and implementing improvements. My administration inherited many initiatives and challenges in the midst of addressing COVID-19 and safely returning students, faculty, and staff to campus. During my administration, we will invest in IT security, standardize and consolidate administrative functions, proceed with critical investments, such as the Administrative Transformation Program, and work with the legislature and governor to reduce unnecessary regulation of the UW System while ensuring greater transparency. The audit will help us with these initiatives.

We look forward to reporting to the Joint Legislative Audit Committee by November 13, 2020 on the recommendations regarding IT security and again on January 15, 2021 regarding the remaining recommendations contained in this audit.

Sincerely,

Tommy G. Thompson
President, UW System