# UNIVERSITY OF UTAH

Report on Information Systems Audit
For the Year Ended June 30, 2018

Report No. 18-11

## OFFICE OF THE
## STATE AUDITOR


AUDIT LEADERSHIP:

John Dougall, State Auditor
Ethan Heintzelman, CPA, Data and Technology Audit Director
Doug Seager, CPA, Financial Audit/IS Manager

# UNIVERSITY OF UTAH

REPORT ON INFORMATION SYSTEMS AUDIT
FOR THE YEAR ENDED JUNE 30, 2018

## TABLE OF CONTENTS

OFFICE OF THE
STATE AUDITOR

October 11, 2018

To the Board of Trustees, Audit Committee,
and
Ruth V. Watkins, President
University of Utah

This letter is provided to communicate, at an interim date, control deficiencies identified from our information systems audit procedures at the University of Utah (University) that are weaknesses in internal control. Accordingly, this communication is based on our audit procedures performed through June 30, 2018. Because we have not completed our financial audit of the University, additional weaknesses may be identified and communicated in our final report.

In planning and performing the information system audit procedures related to our financial statement audit for the fiscal year ended June 30, 2018, we considered the University's internal control over information systems affecting financial reporting (internal control) to determine the audit procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the University's internal control. Accordingly, we do not express an opinion on the effectiveness of the University's internal control.

A deficiency in internal control exists when the design or operation of a control over financial reporting does not allow management or employees, in the normal course of performing their assigned functions to prevent, or to detect and correct, misstatements on a timely basis. A material weakness in internal control over financial reporting is a deficiency, or a combination of deficiencies, that create a reasonable possibility a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis.

Our consideration of internal control is for the limited purpose described in the second paragraph and would not necessarily identify all deficiencies in the entity's internal control that might be material weaknesses or significant deficiencies as defined above. Given these limitations during this audit, based on the procedures performed through June 30, 2018, we did not identify any deficiencies in internal control that we consider to be material weaknesses. However, material weaknesses may exist that have not been identified.

We did note certain deficiencies which we are submitting for your consideration. These matters are described in the accompanying schedule of findings and recommendations.

The University's responses to our findings are included in the accompanying schedule. The University's responses were not subjected to the auditing procedures applied in the audit and, accordingly, we express no opinion on the responses.

The purpose of this interim letter is solely to communicate, prior to completion of our audit, certain deficiencies in internal control applicable to the information systems audit procedures we performed. Accordingly, this communication is not suitable for any other purpose.

Sincerely,

Ethan Heintzelman, CPA, CISA
Data and Technology Audit Director
385-256-8294
eheintzelman@utah.gov

cc: John E. Nixon, Chief Business Officer
Jeffrey J. West, Associate Vice President for Financial and Business Services
Laura M. Howat, Controller & Director, Financial Management
Stephen Hess, Chief Information Officer
Ken Pink, Deputy Chief Information Officer
Randy Arvay, Chief Information Security Officer
Daniel Thornley, Associate Director IT

# FINDINGS AND RECOMMENDATIONS

## 1. LACK OF DOCUMENTATION SHOWING TIMELY DISABLING OF TERMINATED USER ACCOUNTS (Design Deficiency)

We reviewed the PeopleSoft user accounts associated with 25 terminated employees. Although all the accounts were disabled, we could not determine if the accounts were disabled in a timely manner. All system user accounts associated with terminated employees should be disabled as close to the termination date as feasible. There should also be evidence showing when the accounts were disabled. When user accounts associated with terminated employees are not disabled in a timely manner, the risk of improper system access is increased.

**Recommendation:**

**We recommend that the University disable terminated user accounts timely and document when the accounts were disabled.**

*University's Response:*

*University IT already tracks all emails and forms requesting deletions. For an immediate short term solution, from this time forward, we will send and track emails confirming when access is removed. In this way, the request to remove and the completion of removal will both be tracked and saved for reference.*

*One of our major steps in removing access for a user is to delete the entire User Profile from PeopleSoft. So our next phase of this solution is to research and implement turning on database table auditing to track when updates are made to remove User Profiles in PeopleSoft. This will give an accurate time-stamp of when a deletion has taken place.*

*The University of Utah is implementing a third-party governance tool that will track (through standard service tickets) when access for a user is requested to be removed and when removal was accomplished. It is estimated that this tool should be implemented as the primary/final solution sometime in the next 12 to 24 months.*

## 2. INADEQUATE REVIEW OF APPLICATION USER PRIVILEGES (Design Deficiency)

The University's periodic review of PeopleSoft application user privileges is not adequately designed to ensure that all access is necessary and appropriate and that inactive accounts are disabled. Additionally, department heads review their own access to the application. Without a properly designed review, the risk of unauthorized or inappropriate application access is increased.

**Recommendation:**

**We recommend the University establish a more formal process to periodically (e.g. semi-annually) review PeopleSoft application user privileges in order to 1) ensure all application access is necessary and appropriate, 2) detect and disable accounts that are not being used, and 3) ensure end users are not the sole reviewers of their own access.**

*University's Response:*

*University IT currently runs quarterly audits of all PeopleSoft Users that they grant access to. We do not audit users with the default role 'PeopleSoft User' as this role does not give access to any PeopleSoft data. For the short term solution, going forward, we will send an additional email to our Data Stewards (Managers authorizing the users in their areas) for their review. In this way, an authorized non-IT party will verify the appropriateness of all user's access.*

*The University of Utah is implementing a third-party governance tool that will generate quarterly audits wherein all managers will verify the appropriateness of the elevated access of each of their team members. This tool will then track the approvals of access, request removals of access that are inappropriate through standard service tickets, and track all of those actions. It is estimated that this tool should be implemented as the primary/final solution sometime in the next 12 to 24 months.*

## 3. INSUFFICIENT REVIEW OF THE DATABASE AND SERVER USER PRIVILEGES

(Design and Operation Deficiency)

The University does not have a process to periodically review the PeopleSoft database and server user privileges to ensure that all access is necessary and appropriate and that inactive accounts are disabled. Without this review, the risk of unauthorized or inappropriate database and server access is increased.

**Recommendation:**

**We recommend the University establish a process to periodically (e.g. semi-annually) review PeopleSoft database and server user privileges in order to 1) ensure all database and server access is necessary and appropriate, 2) detect and disable accounts that are not being used, and 3) ensure end users are not the sole reviewers of their own access.**

*University's Response:*

*Database User Privileges: Currently, at the beginning of each month, database user audit reports are produced for select PeopleSoft databases. These reports are submitted to the PeopleSoft Application Security Administrator. DBAs also have the ability to provide on-demand reports for any databases within the environment.*

*For future reviews, DBAs will coordinate with USS to perform semi-annual review of database accounts. DBAs will perform the initial review and submit the audit report to the PS Application Security Admin for a secondary review. The PS Application Security Admin will be responsible for notifying the DBAs of any database user accounts that require removal. The review process will be documented and stored in a designated location. In addition, findings and documentation that a review was completed will be recorded.*

*Server User Privileges: Currently, server user privileges are reviewed during any personnel/role change within the Software Platform Services PeopleSoft teams.*

*Moving forward, the server user privileges will be reviewed semi-annually. The Software Platform Services team will perform the initial review. A final review will be conducted by a designated member from the Hardware Platform Services team. The review process will be documented and stored in a designated location. In addition, findings and documentation that a review was completed will also be recorded.*

## 4. INADEQUATE EVIDENCE OF DATA RESTORATION (Design Deficiency)

The University does not document tests of data restorations from backups, as such we could not validate that this control takes place. Tests of data restorations should be done regularly and documented to ensure the process is functioning. Without this review and documentation, the risk of unsuccessful restoration, system unavailability, and data loss is increased.

**Recommendation:**

**We recommend the University formally review and document the test of data restorations from backup to ensure continuity of operations.**

*University's Response:*

*All production databases are currently being restored from backup annually for testing purposes. Results of these restorations are already being documented and include the name of each database, its size, the elapsed time for restoration and specific notes about the environment as applicable. This annual restoration and testing is typically completed around September/October after the start of school.*

*Moving forward, the database restoration testing and review process will be documented and stored in a designated location. Following verification that the database restoration was good, the University UIT USS QA group will do a verification test to make sure the restored data is valid for the associated applications. Results of the application testing will also be documented and stored in a designated location. Additionally, these database restorations and verifications will be scheduled and tracked on the University IT coordination calendar.*