INTERNAL AUDIT REPORT

ERP Information Technology General Controls

R-17-10

October 9, 2017

Contains sensitive security information that should not be publicized pursuant to Utah Code 63G-2-106 and 63G-2-305(12). Such information is also controlled under 49 CFR parts 15 and 1520 and may not be released without appropriate authorization. This information is highlighted in yellow in the internal version of the Report and should be redacted from any public version of this Report.

Audit key:
In order to protect sensitive security information, the following key is provided:
ERP = [redacted]

Executive Summary

Introduction

Internal Audit (IA) has been directed by the Board to perform an internal audit on ERP Information Technology General Controls (ITGCs) to determine if controls are designed adequately and operating effectively to ensure compliance with Utah Transit Authority (UTA) policy and goals. The preliminary stage of the audit was concluded on December 12, 2016 and the audit report was finalized in September 2017.

Objectives and Scope

The primary objective of the audit was to assess whether adequate controls are in place and have been operating effectively for the following areas:

- User Procedures
- Data Security
- System Development and Programming
- Change Management
- Application Support
- Third Party Service Providers

The following areas were excluded from the scope of the ITGC audit because they were covered in previous audits:

- Physical Security
- Environmental Controls
- Backup and Recovery
- Contingency Planning

The period of the preliminary audit was from September 1, 2015, through August 31, 2016 with completion of the audit work focusing on the period of March 31, 2017 through July 31, 2017.

Audit Conclusion

Audit Report Rating*	
The audit revealed that a corporate policy was in place, which included assignment of ownership and responsibility for technology and applications as well as individuals and IT-related working groups. IA also found that the Information Technology Department (IT) has established written procedures for planning, budgeting, and tracking IT training, and aligned the budgeted expenditure accordingly. At the time of our fieldwork, IT was working with Continuous Improvement to implement the record keeping and tracking described. IT had developed and established other recommended policies as well, such as change management and access controls. The upgrade of the ERP is anticipated to be complete in October 2017. In weighing the risks, costs, and benefits, IT Management elected to postpone recommended changes that directly impact the ERP, such as monitoring for appropriate segregation of duties, until such time as the upgrade was complete. Once the upgrade has been completed these recommendations will be addressed. While this report details the results of the audit based on limited sample testing, the responsibility for the maintenance of an effective system of internal control and the prevention and detection of irregularities and fraud rests with management.	

* Refer to Appendix 2

Internal Audit would like to thank the management and staff for their co-operation and assistance during the audit.

Table of Contents

APPENDIX 1

APPENDIX 1

1. Information technology roles and responsibilities

Preliminary Finding R-16-9-1	**High**

Good corporate governance prescribes that ownership and responsibilities be clearly identified and documented for critical processes and assets.
During the audit IA observed the following issues:
a) The ownership of technology and applications between IT and business groups is not clearly documented or understood. [redacted]

Recommendation

Ownership and responsibility for technology and applications should be defined, approved and documented in a corporate policy.

Management Agreement	Owner	Target Completion Date
Agreed	Chief Technology Officer	June 30, 2017

a) A Corporate Policy will be proposed to define the ownership and responsibility for technology and applications by target completion date.
b) An RFP (Request for Proposal) was issued in October 2016 and closed in November 2016. UTA anticipates to complete the upgrade process of all the ERP modules that affect all UTA departments by the end of 2nd quarter 2017.

Final Status	**Implemented**

UTA Corporate Policy No. 2.1.12, "Information Technology Governance," updated as of July 28, 2017, includes assignment of ownership and responsibility for technology and applications as well as individuals and groups. The policy was signed by the UTA President/CEO, and approved as to form by UTA legal counsel.

The ERP upgrade is anticipated to be complete in [redacted]. In weighing the risks, costs, and benefits of implementing controls for other audit findings, such as monitoring for appropriate segregation of duties, IT Management elected to forgo changes to the ERP environment until such time as the upgrade was complete. The decision was documented in a memo addressed to IA, dated May 2, 2017.

Management Agreement	Owner	Target Completion Date
n/a	n/a	n/a

n/a

APPENDIX 1

2. Policies and procedures

Preliminary Finding R-16-9-2	**Medium**

Policies and procedures are in place to establish governance and to provide an organization with sufficient information on the procedures that should be followed to support the execution of the identified processes.

Based on the audit work performed, it was found that:

[redacted]

b) The documents available on the intranet are not limited to the latest versions of the policies and procedures as previous versions are included.
c) Additionally, the audit identified that policies and/or procedures are not in place for the following matters:
   - The ownership of user manuals.
   - [redacted]
   - A prioritization process for the ERP development projects to ensure that resources are used in line with UTA and IT objectives.
   - ERP program development procedures to determine when regression testing or end to end testing is needed for new development or programming changes.
   - ERP programming and development review standards.
   - [redacted]
   - ERP application user support procedures.

[redacted]

Recommendation

a) IT Management should design and implement a periodic review process to assess the existing ERP related policies and procedures for completeness and validity.
b) Additionally, IT Management should oversee the design, documentation, and implementation of departmental policies, including roles and responsibilities, as well as a set of standard operating procedures (SOPs) for the ERP application to address the gaps identified during the review.

Management Agreement	Owner	Target Completion Date
Agreed	Deputy Chief – IS	March 31, 2017

a) IT Management will establish a periodic review of the ERP's policies and procedures to identify gaps.
b) IT Management will establish a working group consisting of IT and super users of the ERP (non-IT departments) to author SOPs and policies to address gaps identified as part of the periodic review of the ERP policies and procedures from comment a) above.

APPENDIX 1

Final Status	Implemented
UTA Technology Office, ERP SOP was adopted in April 2017 and updated and approved by the IT Director on June 21, 2017. The procedure will be reviewed and updated (as needed) on an annual basis.	

Management Agreement	Owner	Target Completion Date
n/a	n/a	n/a
n/a		

3. IT and enterprise governance alignment

Preliminary Finding R-16-9-3	Medium
A governance body is established to govern a specific function and has set objectives. The following governance bodies were established by IT: a) The Technology Advisory Group (TAG) was established with the objective of ensuring a universal review and approval of IT software and technology acquisitions. However, TAG's responsibilities in terms of technology procurements have not been clearly defined in a policy, resulting in the possibility that a function may procure technology equipment without having a clear understanding on TAG's involvement. b) The Technology Awareness Steering Committee (TASC) was established with the objective of ensuring IT review and input of proposed technology projects and development but the governance body's responsibilities are not outlined in a policy.	

Recommendation
The governance bodies' role and responsibilities should be clarified and documented in the policies to provide the business functions with sufficient information in order to ensure compliance with IT's policies. Where other functions support IT in the execution of TAG and TASC's roles, their responsibilities should also be defined and documented in the policies.

Management Agreement	Owner	Target Completion Date
Agreed	Chief Technology Officer	May 31, 2017
IT Management (in consultation with TAG members) will propose a corporate policy to address audit findings with respect to TASC and TAG's roles and responsibilities.		

Final Status	Implemented
UTA Corporate Policy No. 2.1.12, "Information Technology Governance," updated as of July 28, 2017 was adopted and includes assignment of ownership and responsibility for technology and applications as well as individuals and groups. The policy was signed by the UTA President/CEO and approved as to form by UTA legal counsel. Albeit both TAG and TASC committees were disbanded during reorganization efforts and therefore were not referenced in the policy, their previous roles and responsibilities were addressed in Corporate Policy No. 2.1.12.	

APPENDIX 1

Management Agreement	Owner	Target Completion Date
n/a	n/a	n/a
n/a		

4. Employee training

Preliminary Finding R-16-9-4	**High**

Good corporate governance prescribes that a sound training plan is in place for employees to aid in their development and further support a strong control environment.

The audit highlighted the following:

a) Training plans are not recorded for tracking.
b) Training records are not maintained for all IT employees.
c) Follow up for training plan progress is not clearly documented.
d) IA found that IT Management has limited oversight as well as limited monitoring of employee training.
e) Although all employees are required to complete Security Awareness Training IA noted that one of eight Application Support Team members did not complete the annual training in 2015.

Without a system to record employee training plans and track progress IT employees may not receive the training they need resulting in work that does not follow best practices or meet professional standards.

Recommendation

IT Management should establish a process for tracking employee training goals, including dates for completion and follow up.

Management Agreement	Owner	Target Completion Date
Agreed	Chief Technology Officer	February 28, 2017

Management has proposed and approved a preliminary budget for IT training in its FY 2017 budget. IT management will establish a process to enhance the tracking and reviewing employee training progress.

Final Status	**Implemented**

The training process designed has been documented in UTA Information Technology Department Procedure, No. 9.1.0, Technology Training Program, which was updated as of March 2017 and signed by the then IT Acting Director. IT has also aligned budgeted expenditures with training requirements and has designed a process for tracking and monitoring training.

Procedure No. 9.1.0 includes responsibility for planning, budgeting and tracking IT training. At the time of our fieldwork, IT was working with Continuous Improvement to implement the record keeping and tracking described in the procedure developed.

APPENDIX 1

Management Agreement	Owner	Target Completion Date
n/a	n/a	n/a
n/a		

5. Access policies

Preliminary Finding R-16-9-5	**High**
Based on an audit of the ERP Access policies, IA identified the following anomalies: a) From a sample of 25, 1 UTA Security Change form was identified that was not signed by the user's manager as evidence of approval prior to granting ERP access. b) A UTA Security Change form could not be obtained for 4 of a total of 25 test samples due to inadequate document retention.	

Recommendation
IT Management should review the current ERP Access Policies for completeness, validity and clarity to assure that critical control requirements around ERP access are clearly documented. Critical control requirements include, but are not limited to: a) Documented approval by the authorized approver. b) All access forms retained in a well-organized, central repository.

Management Agreement	Owner	Target Completion Date
Agreed	Deputy Chief – IS	March 1, 2017
a) Access will only be granted when a UTA Security Change form is signed by the user's manager and verified by the ERP administrator. b) The approval documents themselves will continue to be uploaded to the document library on SharePoint (Intranet site).		

Final Status	**Low**
ERP SOP No. 11.1.0, was adopted and includes requirements for documented approval and for forms to be retained in a centralized repository. However, one out of four forms sampled during our fieldwork had not been uploaded to the centralized storage location.	

Management Agreement	Owner	Target Completion Date
Yes	IT Director	October 1, 2017
The ERP administrator(s) will be trained and instructed to not grant permissions until a UTA Security Change form is signed by the user's manager and is uploaded to the document library on SharePoint (Intranet site).		

APPENDIX 1

6. End user access review

Preliminary Finding R-16-9-6	High

A process for the review of application access exists to identify and remove inappropriate user access and permissions but the following issues were noted:

a) The access reports provided to the Super Users did not include the users that had access to their areas of responsibility but worked outside of their department.
b) No Super User Access Review was performed for Q2 2016.
c) No set of standards or procedures exist to assist Super Users in performing the quarterly access reviews.
d) The ERP team responsible for sending out User Access Reviews to Super Users is unable to generate one system report of all users and roles, resulting in the super users' reviews being inefficient and difficult as the pertinent information is split into multiple reports, being the responsibilities by roles into one report and the users by roles into other reports.

Recommendation

The ERP Super User Quarterly Access User Review procedures should be formalized to include, but not be limited to:

a) The Super User Quarterly Access User Review's objectives.
b) Super User Quarterly Access User Review's standard procedures that align with the review's objectives.
c) Additionally, the ERP Developers should work with Super Users to determine how best to format user access reports to enable a constructive and efficient review based on the review standards to be developed.

Management Agreement	Owner	Target Completion Date
Agreed	Deputy Chief – IS	April 1, 2017

Documentation of this process will be created outlining this process and its purpose. The current reports will be refined as suggested above.

Final Status	Medium

The ERP SOP No. 11.1.0, included procedures and requirements for a quarterly end user review as well as a privileged user access review.

[redacted]

Management Agreement	Owner	Target Completion Date
Yes	IT Director	[redacted]

[redacted]

APPENDIX 1

[redacted]

7. Technology change control policy

Preliminary Finding R-16-9-7	**Medium**

A process exists to standardize the request, testing, review and approval of the ERP program changes and development.

The audit highlighted the following anomalies:

a) For 1 of 4 ERP Project Promotion Forms selected for testing, the Technology Change Control Board (TCCB) approval documentation could not be found, although the requirement for TCCB approval was documented on the ERP Project Promotion Form.
b) For 2 of 4 ERP changes tested for user testing documentation, the documentation could not be found.
c) For 1 of 4 ERP changes tested for user testing documentation, it has been determined that the testing was performed by the ERP Sr Developer that was also responsible for the programming.
d) For 1 of 4 ERP Project Promotion Forms selected for testing the Technology Change Control Board (TCCB) approval requirement field was missing.
e) Test scripts that guide users in performing a complete and appropriate test of the changes in the ERP are not required or retained.
f) TCCB does not monitor that the change approved was the change that was put into production.
g) IT does not have a documented set of code review standards for programming development.
h) IA noted that there was no monitoring control in place to review the ERP System changes to confirm that all changes were approved.

Recommendation

a) IT Management should explore the possibility of creating a process to electronically document and track ERP promotion forms and TCCB approvals that retains the relevant documentation in a central repository.
b) IT Management should establish a set of standards that guide the requirement, creation, and retention of test scripts for programming changes in the ERP.
c) The TCCB should establish a process to determine that changes put into the ERP production are the changes that were approved for promotion as well as a monitoring control to confirm that all changes were approved appropriately.
d) IT Management should oversee the creation and documentation of a set of code review standards for the ERP program changes.

Management Agreement	Owner	Target Completion Date
Agreed	Deputy Chief – IS	June 30, 2017

a) Technology will investigate a set of tools or process improvements to address this issue. This will occur in Q1-2017.
b) Technology will develop a criteria to determine what changes must be tested by a business department and what changes, due to their technical components, need to be tested by Technology. The criteria will also define how to inform the business that a change is subject to a Technology only test process. This will occur before June 30, 2017.

APPENDIX 1

c) IT Management will establish a TCCB process to determine that changes put into ERP production are the changes that were approved for promotion as well as a monitoring control to confirm that all changes were approved appropriately.
d) Technology will review the current practices and needs and start to define, write and implement a formal change control policy and procedure, including a set of code review standards, which will be appropriate for the Technology staff by Q2-2017.

Final Status	**Medium**

IT has introduced the Point of Business solution to enter, track, document and approve change requests, help desk tickets and incidents.

UTA IT Change Management SOP – TCCB, No. 12.0.1, was approved by IT Management and adopted as of May 31, 2017. IA reviewed the procedure and found that it did include the process for change approval by the TCCB.

UTA Technology Office No. 11.1.0, ERP SOP also included change control such as required approvals, required testing by technology, required code review and required communication with the business units.

Management stated that ERP code is not directly modified by IT staff, and therefore detailed code review standards are not necessary for that application. However, other programs and systems interacting with ERP may need such standards developed. These standards are not incorporated in the current SOPs.

The Applications Support and Development Senior Manager stated monitoring to ensure that all changes put into production were approved will be implemented once the ERP software upgrade is complete and a new monitoring application is implemented.

Management Agreement	Owner	Target Completion Date
Yes	IT Director	October 1, 2017

IT will apply the code review procedure into the TCCB Policy and Procedures to encompass UTA developed (in-house) or modified systems, networks, and programs in order to improve UTA's internal TCCB process.

8. IT segregation of duties

Preliminary Finding R-16-9-8	**Medium**

Segregation of Duties (SOD) is a basic building block of sustainable risk management and internal controls for a business. The principle of SOD is based on shared responsibilities of a key process that disperses the critical functions of that process to more than one person or department. Without this separation in key processes, error and fraud risks are far less manageable.

The audit highlighted the following:
a) Segregations of IT duties are not documented and reviewed periodically.

APPENDIX 1

[redacted]

Recommendation
a) The IT team should perform an annual segregation of duties assessment for ERP related IT responsibilities to ensure that the segregation of duties remain valid, accurate and it is complete. This assessment should be documented and reviewed by IT Management. b) IT Management should establish procedures for acceptable ERP system activity of IT users with elevated access. The procedures should be documented, including what level of access requires monitoring as well as permitted and restricted activities for users with elevated access.

Management Agreement	Owner	Target Completion Date
Agreed	Deputy Chief – IS	March 1, 2017

a) IT Management will perform an assessment on conflicting and sensitive ERP System IT responsibilities (e.g. production/development/QA/database) and identify where segregation of duties can be implemented and where not possible, monitoring controls will be implemented. This assessment will be reviewed at least annually.
b) For IT elevated users, IT Management will identify acceptable and restricted activities with potential consultation outside third party which will then be reviewed IT Management on a periodic basis. Accompanying documentation will be created for this process. IT will explore the possibility of generating automated reports, which would be reviewed by the Application Support and Development supervisors.

Final Status	**Medium**

UTA Technology Office No. 11.1.0, ERP SOP includes independent reviews and approvals prior to advancing changes within ERP environments and required approvals by TCCB.

[redacted]

Management Agreement	Owner	Target Completion Date
Yes	IT Director	[redacted]

[redacted]

APPENDIX 1

[redacted]

Preliminary Finding R-16-9-9
[redacted]

Recommendation
[redacted]

Management Agreement	Owner	Target Completion Date
[redacted]	[redacted]	[redacted]
[redacted]		

Final Status
[redacted]

Management Agreement	Owner	Target Completion Date
[redacted]	[redacted]	[redacted]

APPENDIX 1

[redacted]

10. ERP **risk assessment**

Preliminary Finding R-16-9-10	**Medium**
Risk assessments are prepared to identify potential problems before they occur so that risk-handling activities may be planned and invoked as needed across the function to mitigate adverse impacts on achieving objectives. The IT team prepared an ERP risk assessment in 2015 that included an action plan to address the potential problems in the risk assessment. However, the risk assessment did not include target dates for completion, nor assigned ownership for monitoring of the action plans that were assigned. This resulted in some of the actions agreed upon not executed to address the risks identified.	
Recommendation	
IT management should clearly define dates for completion and identify an owner to follow up on the progress of the recommendations and action plans.	

Management Agreement	Owner	Target Completion Date
Agreed	Deputy Chief – IS	March 31, 2017
An ERP Risk Assessment will be conducted within the first quarter of 2017. Tasks will be assigned to the appropriate personnel and due dates will be set. The progress will be reported to the management team in the monthly IT Security Report. Any task past due will be brought to the attention of IT Management.		

Final Status	**Implemented**
A 2017 ERP Risk Assessment was on file and contained recommendations with owners and target completion dates. IA was able to obtain and review the Security report for June 2017and confirmed that tasks from the ERP risk assessment were included in the report. Passed due action items were noted in red font.	

Management Agreement	Owner	Target Completion Date
n/a	n/a	n/a
n/a		

APPENDIX 1

11. VPN access

Preliminary Finding R-16-9-11	High

VPN access is given to users for access to UTA networks from the outside. VPN access presents additional risk with terminated users who are able to continue accessing UTA applications from outside UTA. During our review of VPN access we noted the following:

a) IA was not able to obtain the ERP UTA VPN Access Request form for 10 of the 25 users selected for testing, which was consistent with management's statement that VPN provisioning procedures were not well formalized prior to 2013.
b) No monitoring control is in place to determine those users whose VPN access should be revoked.
c) From a sample of 25, 1 exception was found where the UTA Employee's VPN Access Request form was missing the first page of the document. The missing page included information on the identity of the employee requesting the VPN access and the manager that approved the access.

Recommendation

a) A process should be established to ensure that all future applications for VPN access follows the appropriate process prior to VPN access granted to users.
b) IT Management should implement a monitoring process that insures the timely removal of VPN access of terminated users.
c) IT Management should confirm that all current VPN users have documented, approved access and that the supporting documentation is available.

Management Agreement	Owner	Target Completion Date
[redacted]	Deputy Chief – IS	February 28, 2017

[redacted]

Final Status [redacted]

IA inspected and determined that UTA Technology Office Procedure, No. 1.2.0, VPN Access Procedure included procedures for granting VPN access and retaining related documentation as well as monitoring VPN access for inactive users.

[redacted]

APPENDIX 1

[redacted]

Management Agreement	Owner	Target Completion Date
[redacted]	[redacted]	[redacted]

12. Monitoring elevated access and IT processes

Preliminary Finding R-16-9-12	High

Good IT governance includes not only generating a report on IT system or application activities performed but also the review of such reports to identify any exceptions and to follow-up on these exceptions. Evidence of review of such exception reports are retained as an audit trail of the execution of the control.

[redacted]

Recommendation

[redacted]

Management Agreement	Owner	Target Completion Date
[redacted]	[redacted]	[redacted]

APPENDIX 1

[redacted]

Final Status	Medium

IA obtained a copy of the UTA Application Support Procedure, No. 11.2.0, Database Procedures and Guidelines and noted that it contained requirements for Database Monitoring.

[redacted]

Management Agreement	Owner	Target Completion Date
[redacted]	[redacted]	[redacted]

13. JD Edwards report creation and modification access

Preliminary Finding R-16-9-13	High

[redacted]

Recommendation

[redacted]

Management Agreement	Owner	Target Completion Date
Agreed	Deputy Chief – IS	December 31, 2016

This recommendation will be communicated to affected users and will be implemented by the end of December 2016.

APPENDIX 1

Final Status	Implemented
[redacted]	

Management Agreement	Owner	Target Completion Date
n/a	n/a	n/a
n/a		

14. Terminated user access

Preliminary Finding R-16-9-14	Medium
[redacted]	

Recommendation
[redacted]

Management Agreement	Owner	Target Completion Date
[redacted]		

Final Status	Medium
[redacted]	

APPENDIX 1

[redacted]

Management Agreement	Owner	Target Completion Date
[redacted]	[redacted]	[redacted]

[redacted]

APPENDIX 2

*REPORT RATING MATRICES

OVERALL REPORT RATING

The overall ratings are defined as follows, applicable to the audit scope as defined

Descriptor	Guide
Fully effective	Controls are as good as realistically possible, both well-designed and operating as well as they can be.
Substantially effective	Controls are generally well designed and operating well but some improvement is possible in their design or operation.
Partially effective	Controls are well designed but are not operating that well. OR While the operation is diligent, it is clear that better controls could be devised.
Largely ineffective	There are significant gaps in the design or in the effective operation of controls – more could be done.
Totally ineffective	Virtually no credible controls relative to what could be done.

DETAILED FINDING PRIORITY RATING

Descriptor	Guide
High	Matters considered being fundamental to the maintenance of internal control or good corporate governance. These matters should be subject to agreed remedial action within three months.
Medium	Matters considered being important to the maintenance of internal control or good corporate governance. These matters should be subject to agreed remedial action within six months.
Low	Matters considered being of minor importance to the maintenance of internal control or good corporate governance or that represents an opportunity for improving the efficiency of existing processes. These matters should be subject to agreed remedial action and further evaluation within twelve months.
Implemented	Adequate and effective management action taken to address the finding noted in the audit report.

APPENDIX 3

DISTRIBUTION LIST			
Name	**For Action[1]**	**For Information**	**Reviewed prior to release**
President/CEO		*	*
General Counsel		*	
Chief Safety, Security & Technology Officer	*		*
Information Technology Director	*		*
Deputy Chief - IS Manager	*		*
Sr. Information Security Admin	*		*
Application Support Team Lead	*		*
Application Development Team Lead	*		*
IT Operations Support Supervisor	*		*
Manager of Human Resources	*		*

[1]For Action indicates that a person is responsible, either directly or indirectly, depending on their role in the process, for addressing an audit finding.