The State Auditor's Office

INFORMATION TECHNOLOGY COMMON AUDIT ISSUES

THE STATE OF TEXAS
STATE AUDITOR

SEPT 2016-DEC 2017

The State Auditor's Office

INFORMATION TECHNOLOGY COMMON AUDIT ISSUES

Overview

This document provides an overview of common IT issues in audit reports the State Auditor's Office (SAO) released from September 2016 through December 2017.

Information technology (IT) serves a critical role in state operations. State agencies and higher education institutions are increasingly reliant on the automated processing of information. It is important that the IT applications that process information have controls to ensure and protect the accuracy, integrity, reliability, and confidentiality of the State's information.

Due to the increased reliance on IT applications, a significant portion of the audits the SAO performs include an IT component. Auditors select IT controls for testing during an audit based on a risk assessment. The risk assessment considers, among other factors, the objectives and scope of the audit. Therefore, the SAO does not test all IT controls in every audit, with the high-risk and high-impact IT controls being tested more frequently. In addition, to minimize security risks, the SAO does not publicly report sensitive IT audit issues, in accordance with Texas Government Code, Section 552.139.

Each report included is hyperlinked to the full report available on the SAO's Web site. Additional reports the SAO has released are available via our online report search tool located at https://www.sao.texas.gov.

First Assistant State Auditor Lisa R. Collier, CPA, CFE, CIDA,
and additional State Auditor's Office personnel are available as a resource
to the Legislature on any of our reports.

State Auditor's Office Contact Information

For additional information regarding any report, please contact:

☎ Verma Elliott, Assistant State Auditor, (512) 936-9500, verma.elliott@sao.texas.gov

🌐 State Auditor's Office Web site: https://www.sao.texas.gov

📍 Address: Robert E. Johnson, Sr. Building, 1501 N. Congress Ave., Austin, TX 78701

The State Auditor's Office

INFORMATION TECHNOLOGY COMMON AUDIT ISSUES

The SAO released 51 audit reports from September 2016 through December 2017 that included IT audit work.

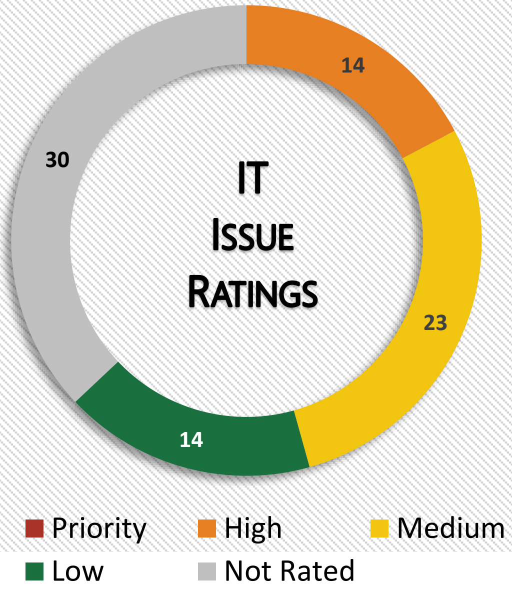
More than half (27 reports) of the SAO audits that included an IT component identified issues in IT controls.

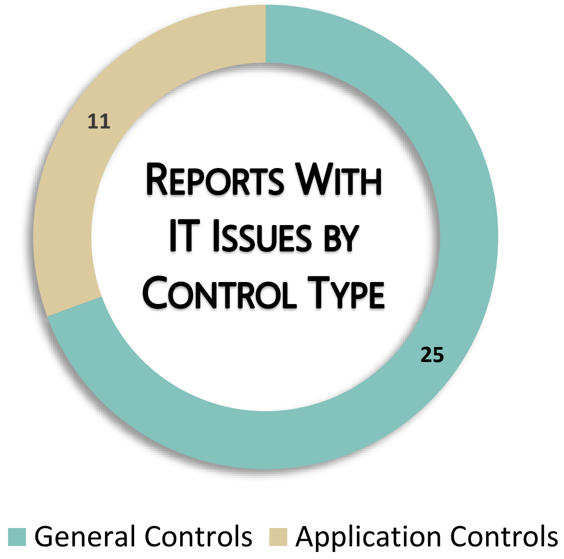
IT issues were prevalent in SAO audit findings, affecting numerous entities, including state agencies, higher education institutions, and non-state entities. In addition, IT issues were identified across all types of audits performed by the SAO, including performance audits, financial audits, and federal compliance audits.

As noted in the IT Issue Ratings graph, almost half (45.7 percent) of the IT issues identified in SAO audit reports released from September 2016 through December 2017 contributed to a high or medium chapter/sub-chapter rating.

In addition, the 30 IT issues in the graph that are not rated were identified in federal compliance, financial, or performance measure audits that use different rating systems prescribed by audit standards or other published guides.

See the Issue Ratings section on page 24 for additional information about the rating categories.





IT controls are classified into two types: general controls and application controls. As shown in the Reports With IT Issues by Control Type graph, of the 27 SAO audit reports that identified IT issues, 25 (92.6 percent) reports included issues with general controls and 11 (40.7 percent) reports included issues with application controls.

Reports are counted in each category if multiple control issues are identified. See the Background—IT Controls (page 1), General Controls (page 2), and Application Controls (page 11) sections for additional information about IT controls and common audit issues identified.

The State Auditor's Office

INFORMATION TECHNOLOGY COMMON AUDIT ISSUES

Table of Contents

The State Auditor's Office

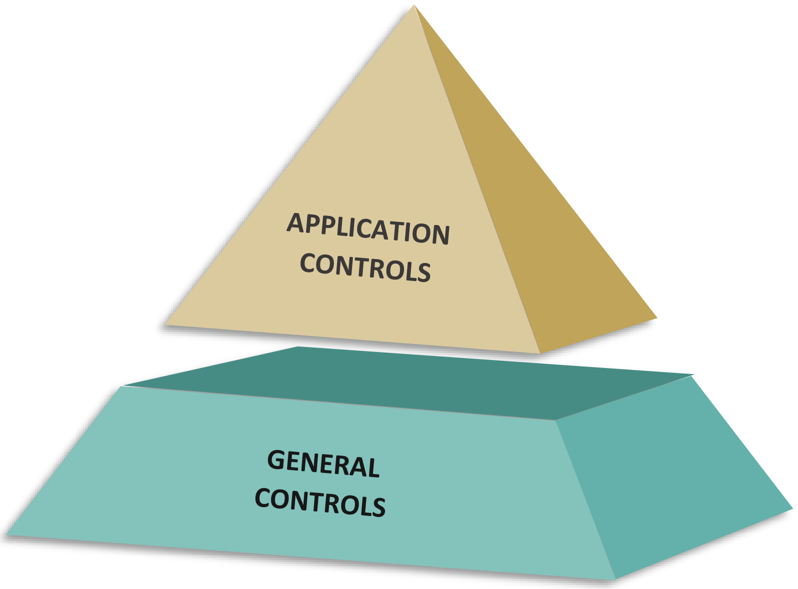
INFORMATION TECHNOLOGY COMMON AUDIT ISSUES

Background—IT Controls

IT controls are classified into two types: IT general controls and IT application controls.

General Controls are broad in scope and relate to the environment in which applications are maintained and operated; therefore, general controls affect all applications. General controls ensure the proper development and implementation of applications and the integrity of program and data files and computer operations *(see the General Controls section on page 2 for additional information)*.

Application Controls are narrow in scope; usually are specific to an individual application; and are designed to ensure that only complete, accurate, and valid data is entered into and processed by an IT application. Application controls address the input, processing, output, and audit trails in an application *(see the Application Controls section on page 11 for additional information)*.



INFORMATION SECURITY STANDARDS

The Department of Information Resources prescribes information security standards for state agencies and higher education institutions in Title 1, Texas Administrative Code, Chapter 202, and its *Security Control Standards Catalog*.

Application controls depend on the reliable operation of the IT environment in which an application operates. Therefore, general control deficiencies in an IT environment can impair the operating effectiveness of application controls.

Other IT-related business processes that exist outside an information system can also impact the data it contains *(see the IT-related Business Processes section on page 15 for additional information)*.

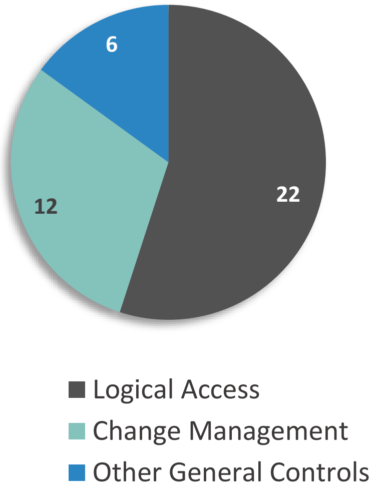
General Controls

Overview

General Controls establish the foundation for information security within the IT environment managed by a state agency or higher education institution. These controls are classified into the following overarching categories:

- **IT Governance**—Information systems strategic plan, the IT risk management process, compliance and regulatory management, and IT policies, procedures, and standards.
- **Logical Access**—Restrict information systems to appropriate personnel and ensure an adequate segregation of duties.
- **Change Management**—Standardized, formal methodology to handle all changes to an information system.
- **Disaster Recovery Planning**—Documented process or set of procedures to recover and protect an agency's or higher education institution's IT infrastructure in the event of a disaster, including backup and recovery.
- **Physical Security**—Safeguard personnel, information, equipment, IT infrastructure, facilities, and other assets.
- **Computer Operations**—Management and monitoring of and response to security; availability and processing integrity events, including incident management; and processing/monitoring of scheduled jobs.
- **Systems Development and Acquisition**—Acquisition or development, implementation, and/or maintenance of IT application systems.

Reports With General Control Issues by Type



Reports are counted above in each category if multiple control issues were identified.

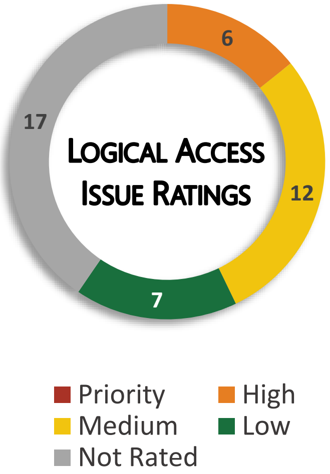
Logical access and change management are the two most common IT general control issues identified in SAO audit reports, as shown in the Reports With General Controls Issues by Type graph. These issues are described in more detail in the following sections.

Other general control issues identified in SAO reports relate to IT governance, disaster recovery planning – backup and recovery, and physical security.

Logical Access

Logical Access controls are a type of general control designed to restrict access to computer software and data files. Logical access controls exist at the server, network, database, and application levels to help restrict information systems to authorized personnel at a level commensurate with their current, approved business needs. Logical access controls include:

- User access
- Periodic user access reviews
- Passwords
- Segregation of duties



IT issues in SAO audit reports that do not receive issue ratings are identified in grey. See the Issue Ratings section on page 24 for additional information about the rating categories.

As shown in the Reports With General Control Issues by Type graph on page 2, the SAO identified issues in logical access controls in 22 audit reports released between September 2016 and December 2017 and these accounted for the greatest number of issues identified for any IT control tested by the SAO during that time period. Of the 42 issues in the Logical Access Issue Ratings graph, 18 (42.9 percent) contributed to a high or medium chapter/sub-chapter rating and 17 (40.5 percent) were not rated, the majority of which related to federal compliance audits. Common issues included:

- Inappropriate user access granted based on job duties and/or access not disabled upon termination of employment.

  Properly implemented user access controls help protect a state entity's data from intentional or accidental disclosure, modification, or erasure, as well as protect the entity's IT resources from misuse.

- Lack of a formal periodic user access review.

  Periodic user access reviews help ensure that access granted and the level of that access continues to be appropriate and required to meet business needs. A user access review should detect inappropriate access.

- Noncompliance with password policies or other best practices.

  Strong password requirements, such as minimum length, expiration after a defined number of days, and complexity, establish the validity of a user's claimed identity and helps safeguard critical IT resources.

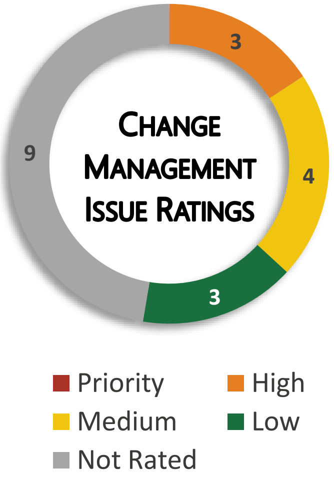
- Lack of adequate segregation of duties.

  User access should be assigned so that no one individual controls all critical stages of a process or transaction. For example, no user should be able to perform all stages within the expenditure process: enter/approve the purchase order, post the receipt, post the vendor invoice, and perform the cash disbursement.

Change Management

Change Management controls are general controls that provide a standardized, formal methodology for processing changes to an application from request through approval to implementation and closure.

Between September 2016 and December 2017, the SAO identified weaknesses in change management controls in 12 audit reports, as shown in the Reports With General Control Issues by Type graph on page 2. Change management represents the second most common SAO IT finding with 19 issues. However, as shown in the Change Management Issue Ratings graph, a smaller portion (36.8 percent) of those issues contributed to a high or medium chapter/sub-chapter rating when compared to logical access issues. In addition, all 9 (47.4 percent of total) change management issues not rated were identified in federal compliance audits. Common issues included:



IT issues in SAO audit reports that do not receive issue ratings are identified in grey. See the Issue Ratings section on page 24 for additional information about the rating categories.

- No formal change management process.

  Entities did not develop, document, and/or implement a change management process to ensure that system changes consistently comply with their policy. Inadequate change management processes can affect system and service availability, such as unplanned system down-time.

- Inappropriate access that permits developers to move their own code to the production environment.

  Segregation of duties was not implemented to help ensure that both unintentional and intentional errors are not introduced into the system. Without adequate segregation of duties, erroneous, fraudulent, or malicious code could go undetected.

- No documented review and approval of changes prior to implementation.

  A documented secondary review and approval process helps to ensure that changes are accurate and receive the appropriate approvals before becoming effective to prevent unintended results from unauthorized changes, errors or omissions in the code, and/or failure to meet key stakeholder needs.

Examples

The following reports include specific examples of **General Controls** issues that the SAO identified during audits. Auditors used professional judgement to rate the audit findings based on the degree of risk or effect of the findings in relation to the audit objective(s) at the chapter/sub-chapter level. Individual control issues contributed to the overall issue ratings listed below. Each report is hyperlinked to the full report and applicable chapter/sub-chapter available on the SAO's Web site.

Parks and Wildlife Department

An Audit Report on Contracting Processes in the Parks and Wildlife Department's Infrastructure Division (SAO Report No. 18-008, December 2017)

HIGH

Most of the Department's Information Technology General Controls Aligned with the Department's Security Policies, But the Department Should Address Certain Access Control Weaknesses

The Department established, reviewed, and approved policies that helped to ensure that its password controls, change management, incident management, backup and recovery, and disaster recovery planning provided adequate guidance for the overall direction and implementation of its information technology security. However, auditors identified certain weaknesses in access controls for the Business Information System (BIS), which the Department used as its financial accounting system.

The report included the following recommendation related to logical access controls.

The Department should strengthen controls to help ensure that users' levels of access are appropriate for their responsibilities. Specifically, the Department should develop and implement security policies and procedures that (1) require periodic user access reviews for BIS and (2) require the Department to maintain information that clearly defines users' roles and responsibilities.

Board of Public Accountancy

An Audit Report on the Board of Public Accountancy: A Self-directed, Semi-independent Agency (SAO Report No. 18-007, December 2017)

HIGH

The Board Should Strengthen Certain Controls Over Passwords, User Access, and Change Management; It Should Also Comply With Certain Requirements in the Texas Administrative Code

Auditors did not identify any significant issues in the reliability of the data in the Board's information systems. However, the Board should strengthen its information technology controls to address significant security risks that could affect the reliability of data used for reporting financial information and performance measure data. To minimize security risks, auditors communicated details about certain significant issues directly to the Board in writing.

The report included the following recommendations related to logical access, change management, IT governance, and other controls.

The Board should:

- Address the weaknesses identified in the password settings for its information systems.
- Develop, document, and implement formal reviews of user access for its information systems, and conduct those reviews at least annually.
- Assign user access rights appropriately based upon users' job responsibilities.
- Develop, document, and implement a formal change management process to help ensure that changes to its information systems comply with its change management policy.
- Review and update its information technology security policies to ensure compliance with the requirements in Title 1, Texas Administrative Code, Chapter 202, and the Department of Information Resources' *Security Control Standards Catalog*.
- Perform and document a risk assessment of its information and information systems as required by Title 1, Texas Administrative Code, Section 202.25, and the Department of Information Resources' *Security Control Standards Catalog*.
- Implement an application control in the AS/400 system to prevent a user from entering a complaint closed date that is prior to that complaint's opened date.

Office of the Comptroller of Public Accounts

An Audit Report on the Office of the Comptroller of Public Accounts' Controls Over the Centralized Accounting Payroll/Personnel System (SAO Report No. 18-002, October 2017)

MEDIUM

The Comptroller's Office Has Implemented Controls Over the Change Management Processes for CAPPS; However, It Should Strengthen Those Controls

The Comptroller's Office should strengthen its change management controls to help ensure that code changes are properly controlled as required by the contract to develop and maintain CAPPS. The Comptroller's Office was unable to provide a complete and accurate population of changes, implemented changes without proper testing that resulted in errors, and lacked documentation related to a sample of changes that auditors reviewed.

The report included the following recommendations related to change management controls.

The Comptroller's Office should:

- Ensure that the change management systems in use effectively track user requests to make changes to the CAPPS system.
- Ensure that the application code used in the process of developing CAPPS system changes to existing production code begins with a copy that mirrors that used in the current production system.
- Ensure that all CAPPS system changes are properly researched, documented, approved, and tested before implementing the changes in the production environment.

Commission on State Emergency Communications

An Audit Report on Selected Contracts at the Commission on State Emergency Communications (SAO Report No. 17-041, July 2017)

MEDIUM

The Commission Should Improve Its Monitoring of Data Security

Auditors identified weaknesses in the Commission's monitoring of data security. Specifically, the Commission did not ensure that user access levels in the Uniform Statewide Accounting System (USAS) enforced appropriate segregation of duties. Additionally, the Commission did not have a process to monitor contractor compliance with contractual data security requirements and did not always follow its policies related to user access to the Poison Control Network.

The report included the following recommendations related to logical access and disaster recovery planning – backup and recovery controls.

The Commission should:

- Configure access levels in USAS to ensure that the same user cannot enter, modify, and release a payment.
- Develop a process to verify contractor compliance with key data security provisions, including the requirement to maintain adequate case management backups.
- Follow its procedures for reviewing and approving user access to the Texas Poison Control Network and performing periodic review of user access.

Texas Facilities Commission

An Audit Report on the Texas Facilities Commission's Compliance with Requirements Related to the Historically Underutilized Business and State Use Programs (SAO Report No. 17-030, April 2017)

HIGH

The Commission Should Strengthen Certain Controls Over Its Information Technology Systems

Auditors identified weaknesses in the Commission's controls over the change management processes for two systems. The Commission's process for making changes to its financial accounting system and legal contracts database does not ensure proper segregation of duties. In addition, auditors determined that the data in the Commission's legal contracts database was unreliable because of incomplete and inaccurate data.

The report included the following recommendations related to change management and other controls.

The Commission should:

- Develop and document a comprehensive change management process that ensures appropriate segregation of duties for its financial accounting system and legal contracts database.
- Implement a process to review the data entered in its legal contracts database for completeness and accuracy.

Health and Human Services Commission

An Audit Report on Human Resources Contract Management at the Health and Human Services Commission (SAO Report No. 17-004, October 2016)

HIGH

The Commission Did Not Adequately Monitor Significant Information Technology Contract Requirements

The Commission should improve its monitoring of the information technology-related requirements in its human resources and payroll services contract. Neither the Commission nor the contractor had an adequate process to periodically review user access to the Commission's human resources system or to ERS Online, which contains confidential employee data, and ensure that user accounts are disabled when users leave employment. In addition, the Commission did not adequately ensure that the contractor complied with information security best practices and the Commission's security protocols and standards as required by the contract.

The report included the following recommendations related to logical access and IT governance controls.

The Commission should:

- Develop, document, and implement a process to periodically review access to CAPPS and ERS Online, and verify that the contractor requests removal of former employees' access to those systems in a timely manner.
- Develop, document, and implement a methodology to monitor the contractor's compliance with the security requirements in the contract, information security best practices, and state and agency-specific requirements. That methodology should include a process to follow up on the results of the monitoring to verify remediation of all issues identified.

Application Controls

Overview

Application Controls are internal controls that usually relate to a specific IT application or system.

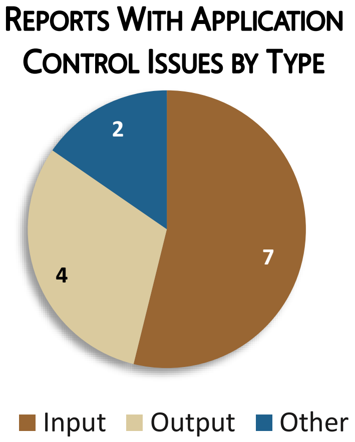
The Department of Information Resources' 2014 *Legacy Systems Study* reported that the State's application portfolio included more than 4,130 IT applications. An IT application is defined by ISACA[1] as a computer program or set of programs that processes records for a specific function. The Centralized Accounting and Payroll/Personnel System (CAPPS) is an example of a state IT application.

Application controls are categorized into the following types:

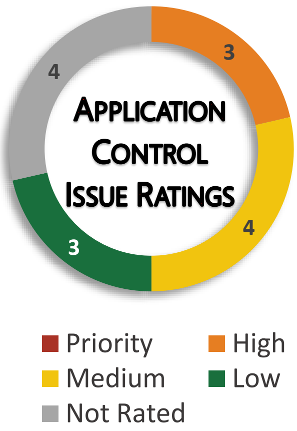
- **Input**—Data entered into an application is accurate, complete, and valid.
- **Processing**—An application's internal processing of data accomplishes the desired tasks and produces the expected results.
- **Output**—System reports and other data extracts are accurate and available only to authorized users.
- **Audit Trail**—A chronological record of system activities to enable the reconstruction and examination of the sequence of events related to transactions in the system.

SAO reports most commonly identify application control issues that relate to input of data into a system, as shown in the Reports With Application Control Issues by Type graph. Other application control issues identified in SAO reports related to processing and output controls. These issues are described in more detail in the following sections.

Of the 14 application control issues identified in the Application Control Issue Ratings graph, 7 (50 percent) contributed to a high or medium chapter/sub-chapter rating.



Reports are counted in each category if multiple control issues are included.



IT issues in SAO audit reports that do not receive issue ratings are identified in grey. See the Issue Ratings section on page 24 for additional information about the rating categories.

[1] *ISACA, formerly known as the Information Systems Audit and Control Association, is an independent organization that develops audit guidance and best practices for information systems.*

Input

Input controls are application controls to help ensure that data entered into an information system is complete, accurate, and valid. For example, an application could require that an employee's retirement date is entered in a valid format and is not prior to the employee's hire date.

Between September 2016 and December 2017, the SAO reported input control issues in 7 audit reports, as shown in the Reports With Application Control Issues by Type graph on page 11. Common issues included:

- Inadequate input controls to prevent inaccurate and/or incomplete data entry.

  Input controls within a system perform automated checks for data reasonableness, format, sequence, and/or validity as it enters the system. For example, an accounting system may have input controls to ensure that transactions recorded are within approved dollar limits and that the amount field accepts only numeric entries.

  Additional input controls can help to ensure that a user enters the required number of characters for a data field, such as a complete Social Security number; dates entered are reasonable; and data is valid by using a pre-defined drop-down menu of approved entries from which a user can select.

Output

Output controls are application controls that help ensure that reports and data exports from an information system are accurate and available only to authorized users.

As shown in the Reports With Application Control Issues by Type graph on page 11, between September 2016 and December 2017, the SAO reported output control issues in 4 audit reports. Common issues included:

- Reports with programming errors that produced incomplete or inaccurate results.

  System reports can be effective in ensuring outputs from a system are complete and accurate; however, errors in the underlying report programming could produce incomplete, inaccurate, and therefore, unreliable results for key stakeholders.

Examples

The following reports include specific examples of **Application Controls** issues that the SAO identified during audits. Auditors used professional judgement to rate the audit findings based on the degree of risk or effect of the findings in relation to the audit objective(s) at the chapter/sub-chapter level. Individual control issues contributed to the overall issue ratings listed below. Each report is hyperlinked to the full report and applicable chapter/sub-chapter available on the SAO's Web site.

Department of Motor Vehicles

An Audit Report on Complaint Processing at the Department of Motor Vehicles (SAO Report No. 17-036, May 2017)

HIGH

The Department Should Address Significant Weaknesses in Access to and the Input of Data Into Its Complaint Tracking Systems

The Department uses two systems to record and track complaint data: (1) the Complaint Management System (CMS) for tracking motor carrier complaints and (2) the Licensing, Administration, Consumer Affairs, and Enforcement (LACE) system for tracking motor vehicle complaints. At the time of the audit, the Department was in the process of replacing LACE; therefore, auditors did not test general controls for that system and were able to perform only limited application control tests.

Auditors identified significant weaknesses in access controls, change management, and application controls for CMS.

The report included the following recommendations related to input and other controls.

The Department should:

- Ensure that password controls for its complaint systems comply with Department security policies and industry best practices.
- Disable employees' and contractors' access to its complaint systems promptly upon termination of employment or services.

Recommendations continued:

- Ensure that user access privileges for its complaint systems align with users' job duties, and promptly modify user access privileges when users' job duties change.
- Adequately restrict access to complaint system servers.
- Remove access that allows developers to move their own code into the production environment.
- Ensure that its complaint systems contain the applications controls necessary to ensure data integrity and appropriate segregation of duties related to complaint processing.

Credit Union Department

An Audit Report on the Credit Union Department: A Self-directed, Semi-independent Agency (SAO Report No. 17-014, December 2016)

LOW

The Department Accurately Calculated All Three Performance Measures Tested; However, It Should Improve Certain Controls to Ensure That It Continues to Accurately Calculate the Performance Measures Audited

The Department accurately calculated all three performance measures that auditors selected for testing: (1) Percentage of Credit Unions Receiving Regular Examination Annually, (2) Percentage of Reports to Credit Unions Within 20 Days, and (3) Percentage of Complaints Investigated and Responded to Within 30 Days of Receipt.

The report included the following recommendations related to output and other controls.

The Department should:

- Update programming in ACT! for performance measure reports to ensure that all applicable credit unions are included.
- Develop, document, and implement a formal review process to verify that it uses the correct data in performance measure calculations and that it uses the approved methodology when performing the calculations.

IT-related Business Processes

IT-related Business Processes can establish controls that exist outside an information system but that affect the data the system contains. Those processes often include a manual component that agency or higher education institution personnel perform and are designed to prevent, or detect and correct, errors and omissions. Inadequate IT-related business processes could result in information systems containing inaccurate and/or incomplete data.

The SAO identified weaknesses in IT-related business processes in several audit reports released between September 2016 and December 2017. Common issues included:

- No formal process and/or procedures over data entry and edits.

  Documented policies and procedures help standardize the data entry process across an organization and provide personnel with adequate guidance to help minimize data entry errors. For example, documented procedures could help ensure that inventory personnel choose the correct asset code when entering an asset into an inventory system.

- No required secondary review of data preparation and/or entry.

  A secondary review by a supervisory individual helps identify and correct data errors or omissions prior to and after being entered and processed by an application.

- No reconciliation of transactions processed.

  Periodic reconciliations of data from different sources can identify discrepancies between systems and help to ensure that the data processed and recorded in multiple systems is complete and accurate. For example, an agency or higher education institution may perform periodic reconciliations of the transactions recorded in its internal accounting system to the transactions that it reports in the Uniform Statewide Accounting System.

Audit Reports—IT Issues

The State Auditor's Office released 51 audit reports that included an IT component between September 2016 and December 2017. When applicable, IT control weaknesses in each report are noted below. Individual control weaknesses contributed to the overall chapter/sub-chapter issue ratings and the highest rating included in the report for each control category is listed.

Report Title	Report Number	Release Date	— General Controls —			Application Controls
			Logical Access	Change Management	Other	
A Report on the Audit of the Permanent School Fund's Fiscal Year 2017 Financial Statements	[18-013]	12/29/2017				
A Report on the Audit of the Department of Housing and Community Affairs' Fiscal Year 2017 Financial Statements	[18-012]	12/29/2017				
A Report on the Audit of the Employees Retirement System's Fiscal Year 2017 Financial Statements	[18-011]	12/29/2017				
An Audit Report on Financial Processes at the Military Department	[18-010]	12/22/2017				

See the Issue Ratings section on page 24 for additional information about the rating categories.

Report Title	Report Number	Release Date	— General Controls —			Application Controls
			Logical Access	Change Management	Other	
An Audit Report on Performance Measures at the Cancer Prevention and Research Institute of Texas	18-009	12/20/2017	●			●
An Audit Report on Contracting Processes in the Parks and Wildlife Department's Infrastructure Division	18-008	12/15/2017	🟠			
An Audit Report on the Board of Public Accountancy: A Self-directed, Semi-independent Agency	18-007	12/15/2017	🟠	🟠	🟠	🟠
An Audit Report on the Audit of the Teacher Retirement System's Fiscal Year 2017 Financial Statements	18-005	11/27/2017				
An Audit Report on On-site Financial Audits of Selected Residential Foster Care Contractors	18-004	10/31/2017	🟡			
An Audit Report on the Office of the Comptroller of Public Accounts' Controls Over the Centralized Accounting Payroll/Personnel System	18-002	10/13/2017		🟡		🟡
An Audit Report on Incentive Compensation at the Permanent School Fund, General Land Office, Employees Retirement System, and Teacher Retirement System	18-001	09/21/2017				

Report Title	Report Number	Release Date	— General Controls —			Application Controls
			Logical Access	Change Management	Other	
An Audit Report on Financial Processes at the Office of Court Administration	17-048	08/31/2017				
An Audit Report on Selected Facilities Funding Programs at the Texas Education Agency	17-046	08/24/2017				
An Audit Report on Grant Management at the Soil and Water Conservation Board	17-045	08/14/2017				
An Audit Report on Selected Major Agreements Under the Texas Economic Development Act	17-043	07/31/2017	●			
An Audit Report on Financial Processes at the Alcoholic Beverage Commission	17-044	07/28/2017	●	●		
An Audit Report on Selected Contracts at Stephen F. Austin State University	17-042	07/27/2017				
An Audit Report on Selected Contracts at the Commission on State Emergency Communications	17-041	07/27/2017	●		●	

Report Title	Report Number	Release Date	— General Controls —			Application Controls
			Logical Access	Change Management	Other	
An Audit Report on Selected Grants to Public Community Colleges at the Texas Workforce Commission	17-040	07/20/2017	🟢			🟡
An Audit Report on Selected Contracts at the Office of the Attorney General	17-039	06/14/2017				
An Audit Report on Selected Contracts at the Department of Information Resources	17-038	06/14/2017	🟢			
An Audit Report on the Audit of Teacher Retirement System's Fiscal Year 2016 Employer Pension Liability Allocation Schedules	17-037	06/05/2017				
An Audit Report on Complaint Processing at the Department of Motor Vehicles	17-036	05/23/2017	🟠	🟠		🟠
An Audit Report on Financial Processes at the Commission on the Arts	17-035	05/19/2017	🟡	🟡		
An Audit Report on the Department of Savings and Mortgage Lending: A Self-directed, Semi-independent Agency	17-034	05/12/2017	🟡		🟡	🟡

Report Title	Report Number	Release Date	— General Controls —			Application Controls
			Logical Access	Change Management	Other	
An Audit Report on Enforcement Activities at the Funeral Service Commission	17-033	05/09/2017				
An Audit Report on Selected Contracts at the Department of Criminal Justice	17-032	05/02/2017				
An Audit Report on the Texas Facilities Commission's Compliance with Requirements Related to the Historically Underutilized Business and State Use Programs	17-030	04/14/2017		●		
An Audit Report on Selected Contracts at the Commission on Environmental Quality	17-029	03/28/2017				
An Audit Report on the University of Texas Medical Branch at Galveston's Compliance with Requirements Related to the Historically Underutilized Business and State Use Programs	17-028	03/20/2017				
State of Texas Federal Portion of the Statewide Single Audit Report for the Fiscal Year Ended August 31, 2016	17-314	02/28/2017	●	●		●
State of Texas Financial Portion of the Statewide Single Audit Report for the Year Ended August 31, 2016	17-555	02/28/2017	●			

The State Auditor's Office

INFORMATION TECHNOLOGY COMMON AUDIT ISSUES

Report Title	Report Number	Release Date	— General Controls —			Application Controls
			Logical Access	Change Management	Other	
A Report on State of Texas Compliance with Federal Requirements for the Student Financial Assistance Cluster for the Fiscal Year Ended August 31, 2016	17-027	02/22/2017	●	●		
An Audit Report on HealthSpring Life and Health Insurance Company, Inc., a Medicaid STAR+PLUS Managed Care Organization	17-025	02/15/2017				🟠
An Audit Report on Certification of the Permanent School Fund's Bond Guarantee Program for Fiscal Year 2016	17-024	02/14/2017				
A Report on the Audit of the Employees Retirement System's Fiscal Year 2016 Pension Schedules	17-021	02/03/2017				
An Audit Report on the University of Texas at El Paso's Compliance with Benefits Proportional Requirements	17-022	02/01/2017				
An Audit Report on the Office of Consumer Credit Commissioner: A Self-directed, Semi-Independent Agency	17-020	01/17/2017	🟡	🟢		🟢
A Report on the Audit of the Permanent School Fund's Fiscal Year 2016 Financial Statements	17-019	01/13/2017				

Report Title	Report Number	Release Date	— General Controls —			Application Controls
			Logical Access	Change Management	Other	
A Report on the Audit of the Department of Housing and Community Affairs' Fiscal Year 2016 Financial Statements	17-018	12/30/2016				
A Report on the Audit of the Employees Retirement System's Fiscal Year 2016 Financial Statements	17-016	12/06/2016				
An Audit Report on the Credit Union Department: A Self-directed, Semi-independent Agency	17-014	12/01/2016	🟡		🟡	🟢
A Report on the Audit of the Teacher Retirement System's Fiscal Year 2016 Financial Statements	17-015	11/30/2016				
An Audit Report on the Department of Banking: A Self-directed, Semi-independent Agency	17-012	11/28/2016	🟢	🟢	🟢	
An Audit Report on On-site Financial Audits of Selected Residential Foster Care Contractors	17-011	10/31/2016				
An Audit Report on the Texas Multiple Award Schedule (TXMAS) Contracts Program at the Office of the Comptroller of Public Accounts	17-010	10/20/2016				🟡

Report Title	Report Number	Release Date	— General Controls —			Application Controls
			Logical Access	Change Management	Other	
An Audit Report on the Department of Public Safety's Compliance with Requirements Related to the Historically Underutilized Business and State Use Programs	17-008	10/13/2016	🟡			
An Audit Report on Medicaid Managed Care Contract Processes at the Health and Human Services Commission	17-007	10/13/2016	🟡	🟡		
An Audit Report on Human Resources Contract Management at the Health and Human Services Commission	17-004	10/10/2016	🟠		🟠	
An Audit Report on Financial Processes at the Department of Licensing and Regulation	17-003	09/16/2016	🟡			
An Audit Report on the Lower Colorado River Authority	17-001	09/01/2016		🟢		

Issue Ratings

Auditors use professional judgement to rate the audit findings identified in certain audit reports. For each report, ratings are determined based on the degree of risk or effect of the findings in relation to the audit objective(s) at the chapter/sub-chapter level.

LOW

The audit identified strengths that support the audited entity's ability to administer the program(s)/functions(s) audited or the issues identified do not present significant risks or effects that would negatively affect the audited entity's ability to effectively administer the program(s)/function(s) audited.

MEDIUM

Issues identified present risks or effects that if not addressed could moderately affect the audited entity's ability to effectively administer program(s)/function(s) audited. Action is needed to address the noted concern(s) and reduce risks to a more desirable level.

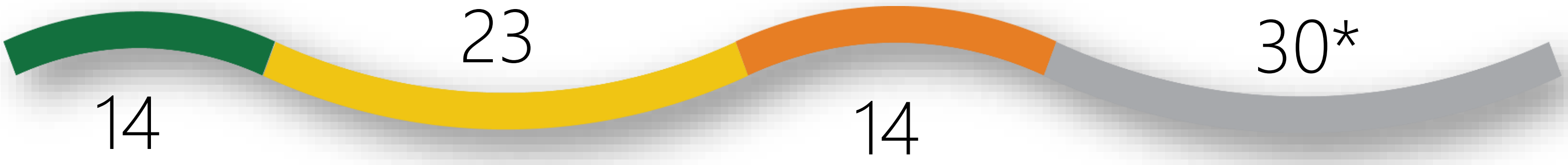
HIGH

Issues identified present risks or effects that if not addressed could substantially affect the audited entity's ability to effectively administer the program(s)/function(s) audited. Prompt action is essential to address the noted concern(s) and reduce risks to the audited entity.

PRIORITY

Issues identified present risks or effects that if not addressed could critically affect the audited entity's ability to effectively administer the program(s)/function(s) audited. Immediate action is required to address the noted concern(s) and reduce risks to the audited entity.

IT Ratings Issued (September 2016-December 2017)



The grey bar represents IT issues in SAO audit reports that do not receive issue ratings.

The State Auditor's Office

INFORMATION TECHNOLOGY COMMON AUDIT ISSUES