Information Technology (IT) – Common Audit Issues

SWIAF/SEIAF – Joint Meeting, Austin, TX

Justin Griffin and Michelle Rodriguez
Texas State Auditor's Office

August 13, 2019

Overview

- Discuss the most common information technology (IT) issues identified in the State Auditor's Office (SAO) audit reports.

- Discuss an approach for dealing with potentially sensitive or confidential IT issues during the SAO's reporting process.

Why are IT controls important?

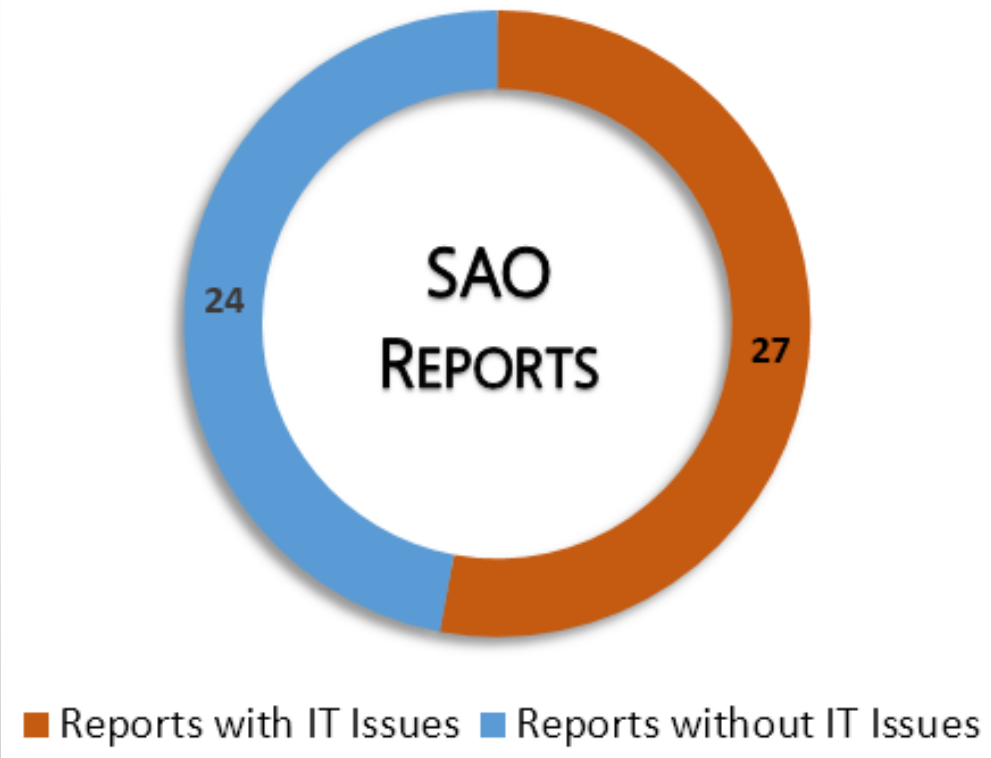
- State agencies and universities are increasingly reliant on the automated processing of information.
- Therefore, it is critical that IT systems that process information have controls to ensure and protect the accuracy, integrity, reliability, and confidentiality of the State's information.
- Due to the ever-increasing reliance on IT applications, a significant portion of the audits the SAO performs include an IT component.

What criteria applies to IT controls?

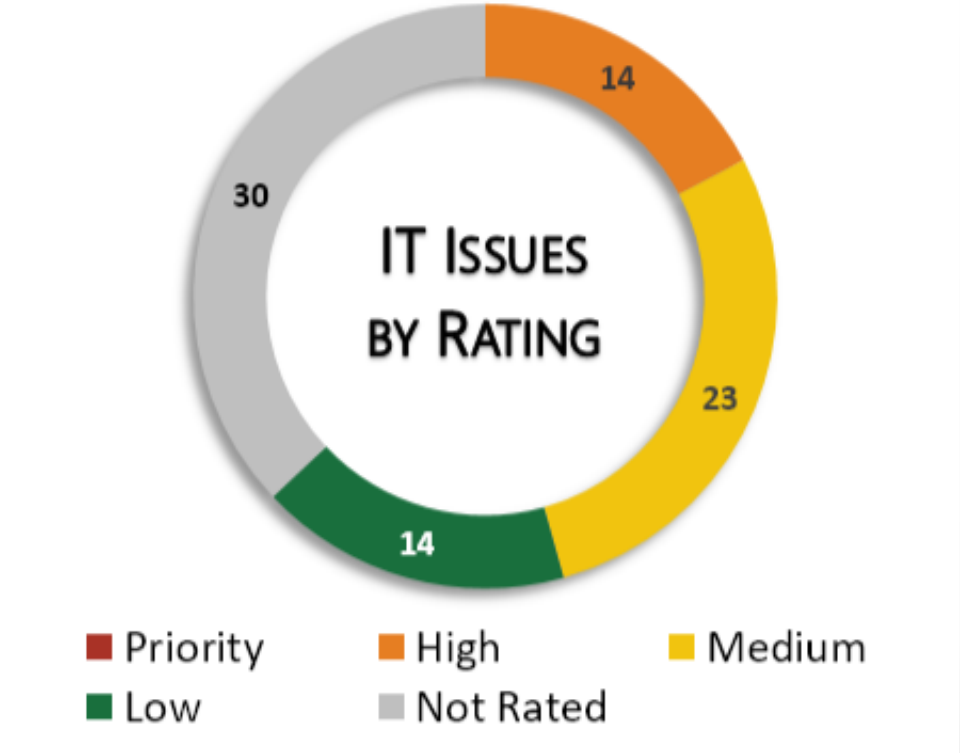
- The Texas Department of Information Resources (DIR) prescribes information security standards for state organizations and universities in Texas.
- DIR has also created a Security Control Standards Catalog (Control Catalog), which aligns with NIST SP 800-53.
- The Control Catalog serves as a baseline of minimum IT controls that state entities must use to provide the appropriate levels of information security according to risk levels.

Frequency of IT Issues

- **The SAO released 51 audit reports from September 2016 through December 2017 that included IT audit work.**
- **<u>More than half</u> of those reports identified IT issues.**



Significance of IT Issues

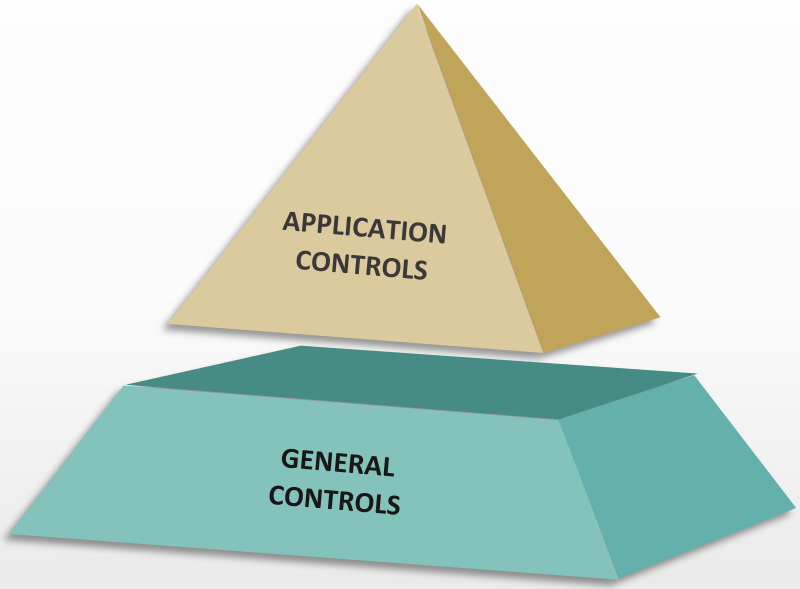


Almost half (46%) of the IT issues identified in SAO audit reports released from September 2016 through December 2017 contributed to a High or Medium chapter/sub-chapter rating.

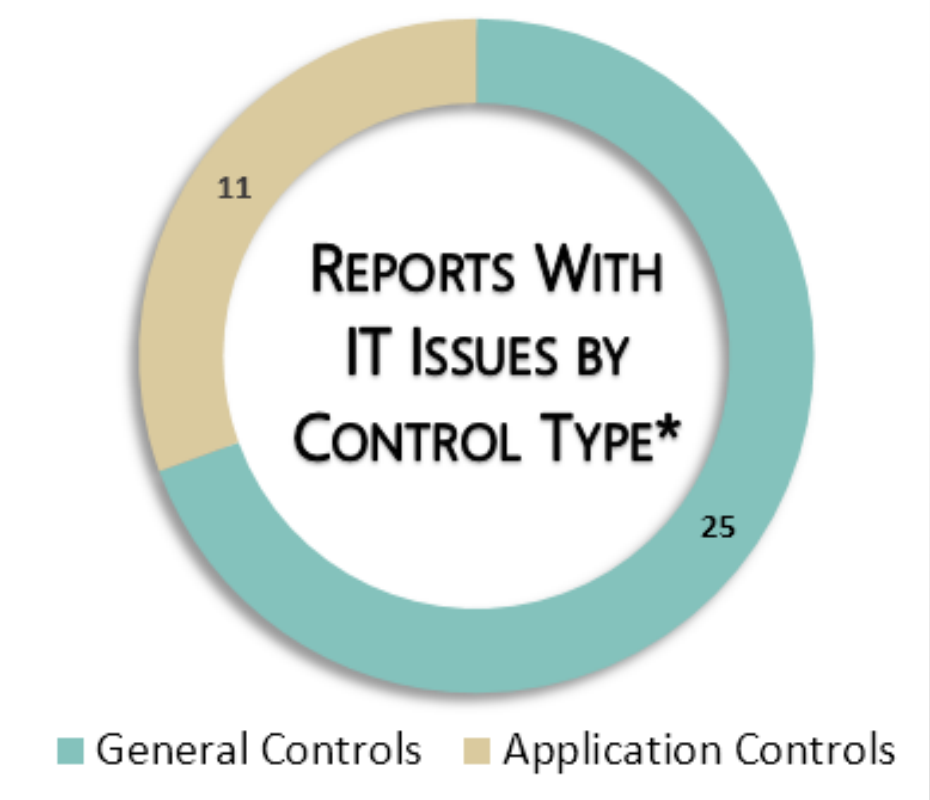
Background—IT Controls

- **IT Application Controls** are narrow in scope, usually are specific to an individual application, and are designed to ensure the complete and accurate processing of data, from input through output.

- **IT General Controls** are much broader in scope and relate to the environment in which applications are maintained and operated; therefore, general controls affect all applications.



General Control Issues
vs.
Application Control Issues



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

IT General Controls

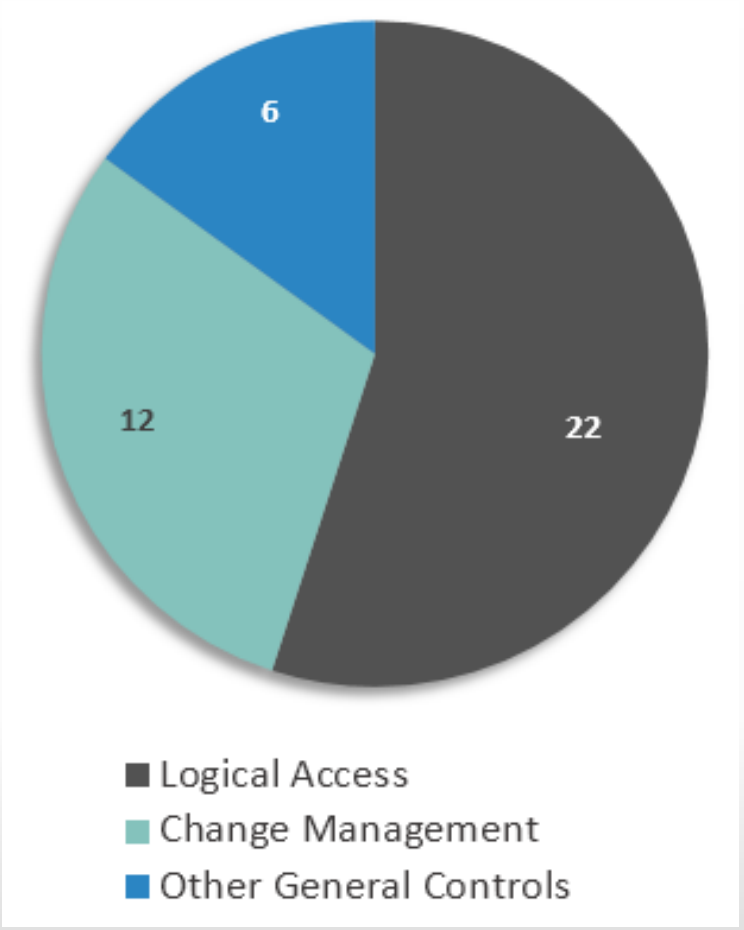
IT General Controls

Logical Access—Restrict information systems to appropriate personnel and ensure an adequate segregation of duties.

Change Management—Standardized, formal process for making changes to an information system.

Other - IT governance, physical security, and disaster recovery planning.

REPORTS WITH GENERAL CONTROL ISSUES BY TYPE



IT General Controls

Common **Logical Access** issues include:

- Inappropriate user access and/or lack of adequate segregation of duties.
- Lack of a formal periodic user access review.
- Noncompliance with password policies or other best practices.

IT General Controls

Common **Change Management** issues include:

- No formal change management policy or procedures.
- No documented review and approval of changes prior to implementation.
- Inappropriate access that permits developers to move their own code to the production environment.

IT General Controls

Other less common IT General Controls issues:

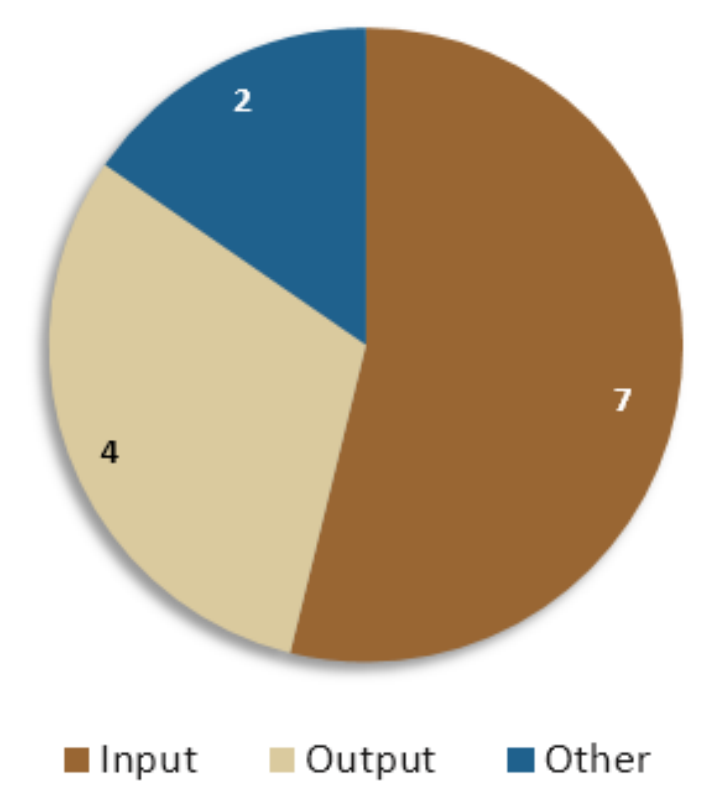
- **IT Governance**—Lack of an IT risk assessment process, inadequate or outdated IT policies and procedures.
- **Physical Security**—Inadequate safeguards for IT infrastructure (typically at a data center) including physical access, fire detection and suppression, backup generators, etc.
- **Disaster Recovery Planning**—Inadequate or outdated disaster recovery plan; the effectiveness of the plan not tested on an annual basis.

IT Application Controls

IT Application Controls

- **Input Controls** ensure that data entered into an application is accurate, complete, and valid.
- **Output Controls** ensure that management reports and other data extracts are accurate and complete.
- **Other**
  - **Processing Controls** ensure that an application's internal processing of data accomplishes the desired tasks and produces the expected results.
  - **Audit Trail Controls** ensure that system activities are recorded to show the sequence of events related to system transactions.

REPORTS WITH IT APPLICATION CONTROL ISSUES BY TYPE



Recap of Common IT Audit Issues

- Most common IT general controls issues:
  - Logical Access (User Access and Passwords)
  - Change Management
- Most common IT application controls issue:
  - Input Controls (edit checks)
- Less common, but no less significant IT issues:
  - Physical Security (Data Centers)
  - Disaster Recovery Planning

Reporting Confidential IT Issues

Overview

Discuss the Texas State Auditor Office's approach for dealing with potentially sensitive or confidential IT issues during the SAO's reporting process.

- Criteria
- Decision makers
- Deliverables
- Stakeholders

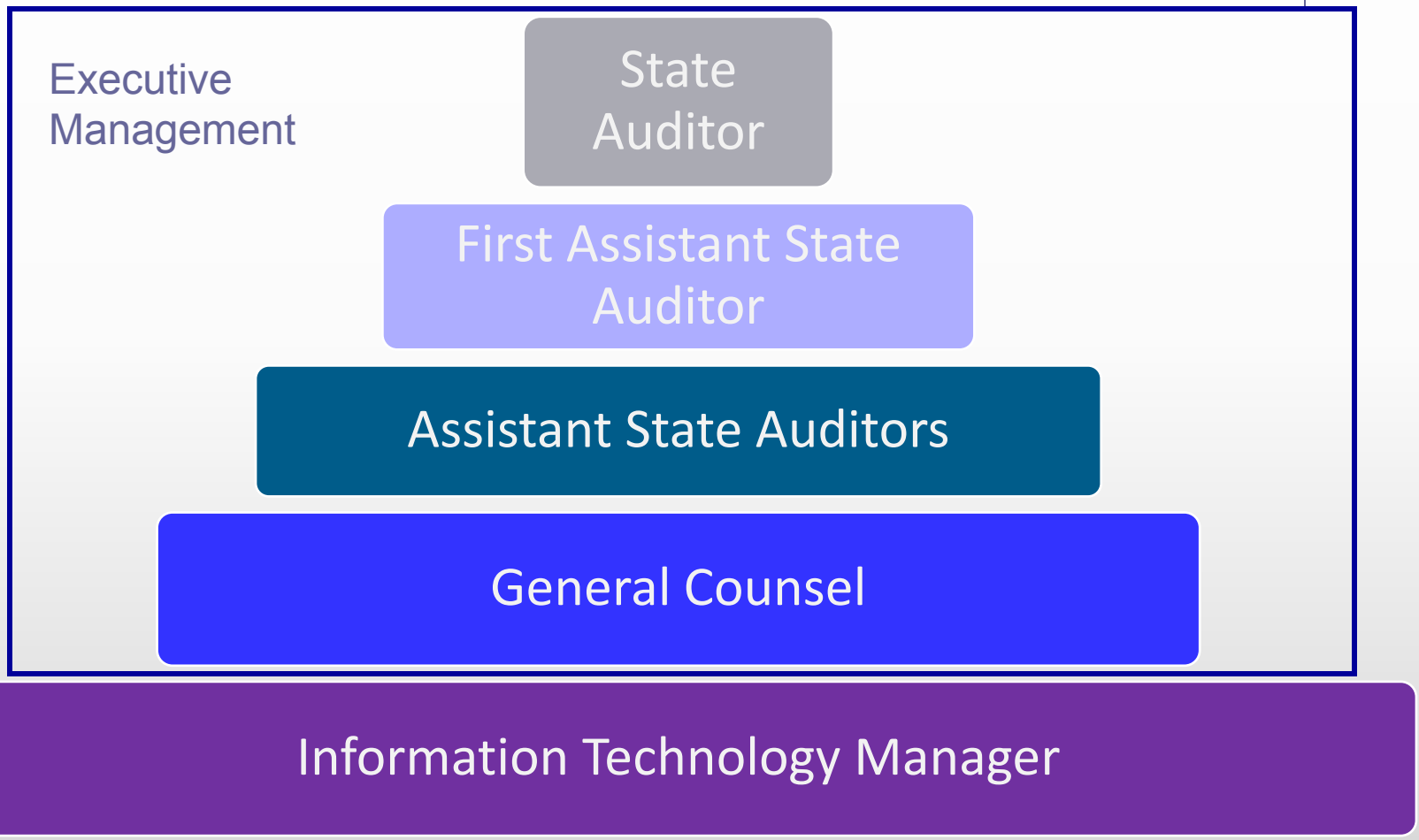
Factors Considered

- Do the issues identified present risks or effects that if not addressed could **substantially or critically affect** the agency's ability to effectively administer the program/function audited?
- Is **prompt or immediate action** required to address the noted concern and reduce risks to the organization? If unmitigated, could these risks or effects lead to:
  - substantial or severe financial loss;
  - inability to accomplish program/function objectives;
  - serious reputation damage; and/or
  - serious violation of policies and procedures, statute, rules, or regulations?

Examples of Significant IT Issues

- Logical Access
  - Not restricting level of access to users or ensure proper segregation of duties.
- Disaster Recovery Plan
  - Not having one.
  - Not having a process to update one.
  - Not testing business continuity or disaster recovery.
- Physical Security
  - No server room cameras.
  - Inability to track access to server room.

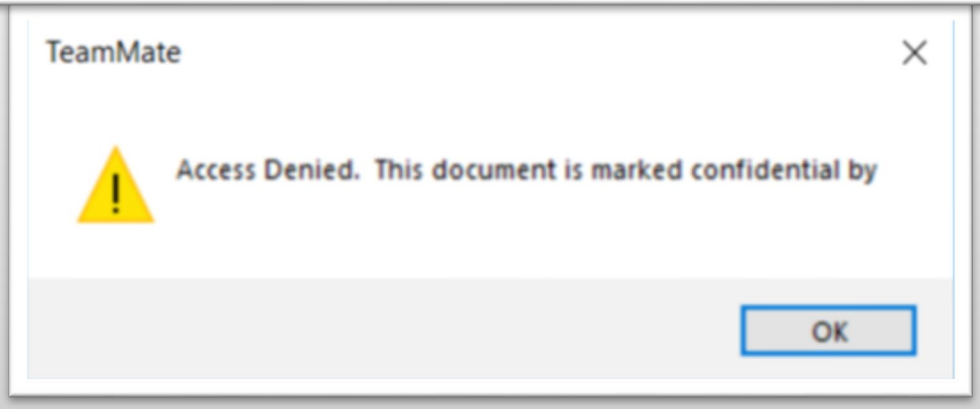
Decision Makers



Confidential Report - Draft

Auditors also identified instances in which the Agency did not adequately restrict the level of access granted to users or ensure a proper segregation of duties. Specifically:

- **System #1.** For X of X users, the role granted to the user was not necessary for the user's job duties. In addition, X of X users had access to both enter and release financial transactions, and the Agency had not implemented mitigating controls to ensure that those transactions were appropriate.
- **System #2.** The Agency did not have documentation describing the functions for X of the X user roles assigned to the Agency's X system users. All X users were assigned to at least X of those X roles. As a result, auditors were unable to determine whether that access was appropriate.



What Criteria Applies to Confidential Information?

- 2018 U.S. Government Accountability Office's *Government Auditing Standards*
  - Standard 9.66 (performance audits)
  - Standard 6.68 (financial audits)

Provides an option for auditors to report confidential information separate from the publicly available report in which auditors identify public safety, privacy, or security concerns.

Criteria Continued

- 2018 U.S. Government Accountability Office's *Government Auditing Standards*
  - Standard 9.61 (performance audits)
  - Standard 6.63 (financial audits)

Require auditors to disclose in the public report that certain information was not included in the public report and the reason for that omission.

Texas Government Code, Section 552.139

EXCEPTION: CONFIDENTIALITY OF GOVERNMENT INFORMATION RELATED TO SECURITY OR INFRASTRUCTURE ISSUES FOR COMPUTERS.

The following information is confidential:

"(2) any other assessment of the extent to which data processing operations, a computer, a computer program, network, system, or system interface, or software of a governmental body or of a contractor of a governmental body is **vulnerable to unauthorized access or harm**, including an assessment of the extent to which the governmental body's or contractor's electronically stored information containing sensitive or critical information is **vulnerable to alteration, damage, erasure, or inappropriate use;"**

Example of a Publicly Released Audit Report

Chapter 2

The Department Should Improve Controls Over Access to Its Driver License System to Prevent and Detect Inappropriate Use of Driver License Data

Chapter 2 Rating:

Priority [2]

Auditors identified significant weaknesses in the Department's controls over access to the information in its Driver License System. In addition, the Department did not have a sufficient process in place to detect employee misuse of the driver license information. To minimize security risks, auditors communicated details about the identified weaknesses related to access, employee use of driver license data, and other sensitive information technology issues separately to the Department in writing.

Example of a Publicly Released Audit Report Continued

Chapter 2

The Department Should Improve Controls Over Access to Its Driver License System to Prevent and Detect Inappropriate Use of Driver License Data

Chapter 2 Rating:

Priority [2]

Auditors identified significant weaknesses in the Department's controls over access to the information in its Driver License System. In addition, the Department did not have a sufficient process in place to detect employee misuse of the driver license information. To minimize security risks, auditors communicated details about the identified weaknesses related to access, employee use of driver license data, and other sensitive information technology issues separately to the Department in writing.

Pursuant to Standard 7.41 of the U.S. Government Accountability Office's *Government Auditing Standards*, certain information was omitted from this report because that information was deemed to present potential risks related to public safety, security, or the disclosure of private or confidential data. Under the provisions of Texas Government Code, Section 552.139, the omitted information is also exempt from the requirements of the Texas Public Information Act.

Confidential Report: Delivery

To obtain management responses from the agency, project management delivers draft copies of the report via:

- Hand delivery of hard copy,

- Secure file sharing system MOVEit, or
- Certified mail.

Final Confidential Report Distribution

Who needs to know?

Agency Management

- Agency head
- Board chair or audit committee chair
- Agency internal audit director

Those Charged with Governance, such as:

- Legislative Committees
- Oversight Committees

Takeaways

Do not expose the agency's technological vulnerabilities to the general public, increasing the likelihood of a cyberattack and/or physical destruction of IT resources.

Do not put the agency in a worse position than it is already in.

Questions?

Justin Griffin

Managing Senior Auditor (Texas State Auditor's Office)

Michelle Rodriguez

Senior Auditor (Texas State Auditor's Office)