

Internal Audit

**Fiscal Year 2017
Internal Audit Annual Report**

17-303

October 2017



Department of Information Resources

Internal Audit Mission Statement

Collaborate with DIR leadership to fulfill the agency's core mission by providing independent and objective audit services designed to add value and improve the effectiveness of risk management, control, and governance processes.

DIR Internal Audit

Lissette Nadal, CIA, CISA, CRISC, Director, Internal Audit

Catherine (Cathy) J. Sherwood, CPA, CITP, CISA, Senior Auditor

Table of Contents

Background	1
Objective	1
Acknowledgement.....	1
Detailed Results	2
I. Compliance with Texas Government Code, Section 2102.015.....	2
II. Internal Audit Plan for Fiscal Year 2017	2
III. Consulting Services and Non-Audit Services Completed	5
IV. External Quality Assurance Review (Peer Review).....	10
V. Internal Audit Plan for Fiscal Year 2018.....	11
VI. External Audit Services Procured in Fiscal Year 2017	15
VII. Reporting Suspected Fraud and Abuse.....	15
Appendix A: Report Distribution	17

Background

The Texas Internal Auditing Act (Texas Government Code 2102) requires certain state agencies like the Department of Information Resources (DIR) to submit an Internal Audit Annual Report each year to the Governor, the Legislative Budget Board, the Sunset Advisory Commission, the State Auditor's Office (SAO), and the entities' governing boards and chief executives. The SAO is charged with prescribing the form and content of the annual report.

In compliance with that mandate, the SAO sets forth guidelines to assist state agencies in preparing the Internal Audit Annual Report. The guidelines represent the SAO's minimum requirements and do not preclude DIR from including additional information in its annual report.

Objective

The purpose of the Internal Audit Annual Report is to provide information on the assurance services, consulting services, and other activities of the Internal Audit function and to assist oversight agencies in their planning and coordination efforts.

Acknowledgement

The DIR Fiscal Year 2017 Internal Audit Annual Report has been prepared in accordance with the guidelines prescribed by the SAO, as required.

Detailed Results

I. Compliance with Texas Government Code, Section 2102.015

Compliance with Texas Government Code, Section 2102.015: Posting the Internal Audit Annual Plan, Internal Audit Annual Report, and Other Audit Information on the DIR Internet Web site¹

The Fiscal Year 2018 Internal Audit Annual Plan and the Fiscal Year 2017 Internal Audit Annual Report are posted in the Internal Audit Web Page of the Department of Information Resources (DIR) Web Site along with periodic reports and other DIR-related audit publications by third-parties. Internal Audit annual plans, annual reports, and periodic reports are posted within 30 days of DIR Board's approval.

The DIR Internal Audit Web Page is located at <http://dir.texas.gov/View-About-DIR/Pages/Content.aspx?id=44>.

A detailed summary of any weaknesses, deficiencies, wrongdoings, or other concerns, if any, raised in the Internal Audit Annual Plan or the Internal Audit Annual Report, and a summary of actions taken by DIR to address those weaknesses, deficiencies, wrongdoings, or other concerns, if any, are included in the Fiscal Year 2017 Internal Audit Annual Report.

The information contained in the annual plan or annual report is not excepted from public disclosure.

II. Internal Audit Plan for Fiscal Year 2017

The Internal Audit Annual Plan for fiscal year 2017 was approved by the DIR Board in October 2016. It included the list of audits planned for the fiscal year. The following table includes the completion status of the audit projects planned for the fiscal year, including the completion status, report number, report date, and report title.

¹ House Bill 16 (83rd Legislature, Regular Session) amended the Texas Internal Auditing Act (Texas Government Code 2102) to require state agencies and institutions of higher education, as defined in the bill, to post agency internal audit plans, internal audit annual reports, and any weaknesses or concerns resulting from the audit plan or annual report on the entity's Internet web site within 30 days after the audit plan and annual report are approved by the entity's governing board or chief executive.

Audit Project #	Audit Project Name/ Report Title/ Objective(s)	Status	Report Date
17-100	Assurance Audits – Tier 1		
17-101	<p><i>DCS Vendor Management and Performance</i> (carried forward to Fiscal Year 2018)</p> <p>Objective:</p> <ul style="list-style-type: none"> To determine whether the data center services reported vendor performance complies with established service level agreements. 	In Progress	-
17-103	<p><i>Xerox Print Mail Process</i></p> <p>Objective:</p> <ul style="list-style-type: none"> To assess whether the Data center Services vendors are in compliance with established service level agreements. 	Complete	June 2017
-	<p><i>Capital Complex Telephone System (CCTS) Operations</i></p> <p>Preliminary Objective:</p> <ul style="list-style-type: none"> To assess whether the operations of the CCTS Program are in compliance with applicable state law and regulations. 	Not Started	-
17-102	<p><i>Network Security Operations</i> (carried forward to Fiscal Year 2018)</p> <p>Objectives:</p> <ul style="list-style-type: none"> To assess whether the operations of the DIR network security function are in compliance with applicable state law and regulations, contract requirements, and best practices. Assess the implementation status of the audit recommendations included in Report #13-105: Network Security Operations Audit. 	In Progress	-
	Assurance Audits – Tier 2		
-	<p><i>Statewide Accessibility Coordination Program</i></p> <p>Preliminary Objective:</p> <ul style="list-style-type: none"> To assess whether the DIR Statewide Accessibility Coordination Program is meeting its goals. 	Not Started	-
-	<p><i>The Technology Architecture</i></p> <p>Preliminary Objective:</p> <ul style="list-style-type: none"> To assess whether the DIR Technology Architecture function ensures selected vendors perform services in accordance to the contracted Statement of Work. 	Not Started	-

Audit Project #	Audit Project Name/ Report Title/ Objective(s)	Status	Report Date
17-200	Consulting and Non-Audit Services		
17-202	External Audit Coordination	Complete	N/A
17-201	Management Advisory Project (MAP)	Complete	N/A
-	Workgroups/ Governance Boards	Complete	N/A
-	Reserved for DIR Board and Executive Leadership Projects <i>Note: Budgeted hours were used to complete project # 17-103.</i>	Complete	N/A
17-300	Required Projects		
-	Continuing Professional Education	Complete	N/A
17-301	Follow-up on Audit Recommendations	Complete	N/A
17-302	Fiscal Year 2018 Internal Audit Risk Assessment/ Annual Plan	Complete	October 2017
17-304	Fiscal Year 2017 Internal Audit Annual Report	Complete	October 2017
17-303	Fiscal Year 2017 Internal Audit Annual Assessment	Complete	August 2017

Explanation of Deviations

Tier 1

- DCS Vendor Management and Performance – this assurance audit started in fiscal year 2017. However, due to 1) staffing constraints and the mandated hiring freeze, and 2) re-assignment of resources to project #17-103, the audit could not be completed in the fiscal year.
- Network Security Operations – this assurance audit started in fiscal year 2017. However, due to 1) staffing constraints and the mandated hiring freeze, and 2) delays in the procurement and contracting process for external audit resources, the audit could not be completed in the fiscal year.
- Capital Complex Telephone System (CCTS) Operations – this assurance audit started in fiscal year 2017. However, due to 1) staffing constraints and the mandated hiring freeze, and 2) re-assignment of resources to project #17-103, the audit could not be completed in the fiscal year.

Tier 2

- Statewide Accessibility Coordination Program – based on limited resources no budgeted hours were allocated to complete this Tier 2 assurance audit. The residual risk of this assurance audit was re-assessed during the fiscal year 2018 Internal Audit Risk Assessment.
- The Technology Architecture – based on limited resources no budgeted hours were allocated to complete this Tier 2 assurance audit. The residual risk of this assurance audit was re-assessed during the fiscal year 2018 Internal Audit Risk Assessment.

No additional deviations from the Fiscal Year 2017 Internal Audit Annual Plan were noted or reported.

Internal Audit Process

DIR Internal Audit implements the following audit process to execute the assurance audits included in the annual plan and to comply with auditing standards.



- Obtain background information
- Gain an understanding
- Conduct an Entrance Conference
- Assess risks and controls
- Identify relevant information systems
- Assess data reliability
- Develop Planning Memo
- Develop Fieldwork Program

- Test and analyze
- Prepare routine progress updates
- Develop issues and/or conclusions

- Develop the audit report
- Conduct an Exit Conference
- Obtain management responses

- Obtain management assertions
- Validate status of recommendations

III. Consulting Services and Non-Audit Services Completed

Consulting Services Completed

Consulting services as defined by *The Institute of Internal Auditors (The IIA)* are advisory in nature, and generally performed at the specific request of an engagement client. The nature and scope of the consulting engagement are subject to agreement

with the engagement client. Consulting services generally involve two parties: 1) the person or group offering the advice — the Internal Auditor, and 2) the person or group seeking and receiving the advice — the engagement client.

The DIR Internal Audit Division did not perform consulting services in fiscal year 2017.

Non-Audit Services Completed

Non-audit services are described by *The General Accountability Office (GAO)* as services that support the entity’s operations such as: 1) certain accounting and financial services, 2) assistance services, 3) separate evaluations, 4) certain Information Technology and valuation services, and 5) participation in committees as non-voting members.

The following table includes the non-audit services completed during fiscal year 2017, including the report number, title, objective(s), results, recommendation(s), and report date, if any.

Project #	Title/ Objective(s)	Results/ Recommendation(s)	Report Date
17-200	Consulting and Non-Audit Services		
External Audit Coordination – Internal Audit serves as the liaison and assist with the State Auditor's Office (SAO) and other state external entities with oversight audit and review responsibility.			
17-202	<p><i>Texas.Gov Financial Audit Report for Calendar Year (CY) 2015</i></p> <p>Objective:</p> <ul style="list-style-type: none"> To perform an examination of the vendor’s (NIC) financial statements and accompanying disclosures for calendar year 2016. The audit covers the vendor’s (NIC or Company) finances for the period from January 1, 2016 to December 31, 2016 and a validation of the completeness and accuracy of the 1) state share, and 2) local funds revenue accounts. 	<p>Results:</p> <p>Opinions:</p> <ul style="list-style-type: none"> In the auditors’ opinion, the financial statements referred to present fairly, in all material respects, the financial position of the Company as of December 31, 2016 and the results of its operations and cash flows for the year then ended in accordance with accounting principles generally accepted in the United States of America. In the auditors’ opinion, the schedule referred to presents fairly, in all material respects, the non-USAS revenue (local finds) of the Company for the year ended December 31, 2016, in accordance with accounting principles generally 	July 2017

Project #	Title/ Objective(s)	Results/ Recommendation(s)	Report Date
		<p>accepted in the United States of America.</p> <ul style="list-style-type: none"> In the auditors' opinion, the schedule referred to presents fairly, in all material respects, the state revenue share of the Company for the year ended December 31, 2016, in accordance with accounting principles generally accepted in the United States of America. <p>Recommendation(s):</p> <ul style="list-style-type: none"> None 	
	<p><i>SAO Audit of Selected Contracts at DIR (Report #17-038)</i></p> <p>Objective:</p> <ul style="list-style-type: none"> Determine whether DIR administered certain contract management functions for selected contracts in accordance with applicable requirements. The work includes the automated systems and processes that support the functions being audited at the DIR. 	<p>Results:</p> <ol style="list-style-type: none"> The Department planned, procured, and formed the Atos contract in accordance with applicable requirements, but it should improve certain aspects of its contract oversight. <p>Recommendation(s):</p> <ul style="list-style-type: none"> Update its oversight controls, such as its contract management plan and risk assessment, to ensure that they address all significant requirements in the most current version of the contract. Update Salesforce controls to ensure that a single user cannot make it appear that two different users have reviewed an invoice. Properly restrict access to key network locations where it maintains invoice review spreadsheets. <ol style="list-style-type: none"> The Department planned and formed the C&T contract in accordance with applicable requirements, but it should improve certain aspects of contract 	<p>June 2017</p>

Project #	Title/ Objective(s)	Results/ Recommendation(s)	Report Date
		<p>procurement, oversight, and training.</p> <p>Recommendation(s):</p> <ul style="list-style-type: none"> • Ensure that it scores only vendor proposals for which it has documentation that it received the proposals on or before the date/time specified in the solicitation document. • Accurately describe in its solicitation the methodology it will use to score vendor proposals, and ensure that it consistently follows that methodology. • Develop, document, and implement procedures to monitor its receipt of contractor progress assessment reports related to HUB subcontracting plans. • Develop, document, and implement procedures help ensure contractor compliance with requirements related to the HUB subcontracting plans. • The Department should improve its processes for ensuring that board members promptly receive required training. 	
	<p><i>Federal Compliance Audit – Uniform Guidance (aka 2017 State of Texas OMB A-133 Audit (aka Single Audit)</i></p> <p>Objective:</p> <ul style="list-style-type: none"> • Determine the State of Texas compliance with the compliance requirements described in the OMB Circular A-133 Compliance Supplement that could have a direct and material effect on each of the State’s major federal programs, as of year ending August 31, 2017. 	<p>Results:</p> <ul style="list-style-type: none"> • No issues but verbal comments were reported for the Information Technology (IT) systems audited. These verbal comments are considered confidential and not for public release. <p>Recommendation(s):</p> <ul style="list-style-type: none"> • None 	
<p>Management Advisory Project (MAP) – Internal Audit performs these projects generally at the request of DIR management or the DIR Board, may be required by a law or regulation, may be included in the Internal Audit Annual Plan, or may result from downscaling an assurance audit.</p>			

Project #	Title/ Objective(s)	Results/ Recommendation(s)	Report Date
17-201	<p><i>Data Center Services Consolidation Measurement Report</i></p> <p>Objective:</p> <ul style="list-style-type: none"> To coordinate with DIR and provide guidance on measuring and reporting on 1) the progress of the data center services (DCS) consolidation effort, and 2) the DCS financial performance – cost savings. 	<p>Results:</p> <ul style="list-style-type: none"> In 2016, the DCS program met its consolidation goals: <ul style="list-style-type: none"> Mainframe – 100% consolidated, Print-Mail – 100% consolidated, and Server – 75% consolidated. The comparison of Fiscal Year 2016 appropriations to actual expenditures resulted in a favorable variance of \$24.4 million. The comparison of Fiscal Year 2016 contract base costs to actual expenditures (based on unit rate charges) resulted in a favorable variance of \$11.3 million. Overall DCS customer satisfaction rate increased to 80%. <p>Recommendation(s):</p> <ul style="list-style-type: none"> None 	April 2017
<p>Workgroups/ Governance Boards – Internal Audit participation in workgroups, governance boards, committees as non-voting members.</p>			
-	<p><i>Workgroups/ Governance Boards (Various)</i></p> <p>Objectives:</p> <ul style="list-style-type: none"> To optimize business acumen on the different programs and support functions within DIR. To assist, counsel or advice DIR management to improve the effectiveness of risk management, controls, and governance processes. 	<p>Results:</p> <ul style="list-style-type: none"> N/A <p>Recommendation(s):</p> <ul style="list-style-type: none"> N/A 	-

IV. External Quality Assurance Review (Peer Review)

Overall opinion of the DIR's most recent external quality assurance review. The review was performed by a State Agency Internal Audit Form (SAIAF) team and the letter report was issued December 2016.

State Agency Internal Audit Forum (SAIAF)
Department of Information Resources Internal Audit Department
External Quality Assurance Review – August, 2016

Peer Review Letter Report

December 8, 2016

Ms. Lissette Nadal-Hogan, CIA, CISA, CRISC
Internal Audit Director
Department of Information Resources
300 W. 15th Street, 13th Floor
Austin, Texas 78701

Dear Ms. Nadal-Hogan,

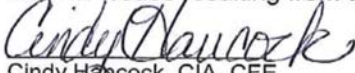
We have completed a Peer Review of the Department of Information Resources for the period August 2015 – August 2016. In conducting our review, we followed the standards and guidelines contained in the Peer Review Manual published by the State Agency Internal Audit Forum (SAIAF).

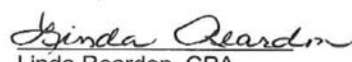
The Institute of Internal Auditors (IIA) *International Professional Practices Framework*, U.S. Government Accountability Office (GAO) *Government Auditing Standards*, and the Texas Internal Auditing Act (Texas Government Code, Chapter 2102) require that Internal Audit functions obtain external quality assurance reviews (peer reviews) to assess compliance with standards and the Act and to appraise the quality of their operations.

We reviewed the internal quality control system of your audit organization and conducted tests in order to determine if your internal quality control system operated to provide reasonable assurance of conformance with the IIA *Standards*, the GAO *Standards*, and the Texas Internal Auditing Act. Due to variances in individual performance and judgment, conformance does not imply adherence to standards in every case, but does imply adherence in most situations.

Based on the information received and evaluated during this external quality assurance review, it is our opinion that the Department of Information Resources' Internal Audit Department receives a rating of "**Pass/Generally Conforms**" and is in compliance with the IIA Standards, the GAO Standards, and the Texas Internal Auditing Act. This opinion, which is the highest of the three possible ratings, means that policies, procedures, and practices are in place to implement the standards and requirements necessary for ensuring the independence, objectivity, and proficiency of the internal audit function.

To the extent lawful, the Department of Information Resources agrees to hold SAIAF and its officers and representatives harmless of any liability arising from the actions of the peer review team or issues resulting from the peer review.


Cindy Hancock, CIA, CFE
Internal Audit Director, TPWD
SAIAF Peer Review Team Lead


Linda Reardon, CPA
Auditor, TWC
SAIAF Peer Review Team Member

V. Internal Audit Plan for Fiscal Year 2018

The Texas Government Code Chapter 2102 (known as the Texas Internal Auditing Act), Subchapter B, §2102.005, Internal Auditing Required, states Internal Audit shall conduct an annual audit plan that is prepared using risk assessment techniques that identify the individual audits to be conducted during the year.

Accordingly, DIR Internal Audit embraces an integrated audit approach to develop its annual risk assessment and annual plan that includes, but is not limited to, strategic, operational, financial, Information Technology (IT), information security, contracting, and the regulatory compliance aspects of the agency.

The following Fiscal Year 2018 Internal Audit Annual Plan is approved by the DIR Board.

Audit Project #	Audit Project Name/ Preliminary Objective(s)	Budgeted Hours*
18-100	Assurance Audits – Tier 1 *	
17-101	<p><i>DCS Vendor Management and Performance</i> (carried forward from Fiscal Year 2017) **</p> <p>Objective:</p> <ul style="list-style-type: none"> To determine whether the data center services reported vendor performance complies with established service level agreements. 	180
17-102	<p><i>Network Security Operations</i> (carried forward from Fiscal Year 2017)</p> <p>Objectives:</p> <ul style="list-style-type: none"> To assess whether the operations of the DIR network security function are in compliance with applicable state law and regulations, contract requirements, and best practices. Assess the implementation status of the audit recommendations included in Report #13-105: CISO/ Network Security Operations Audit. 	300
-	<p><i>Data Center Services Compliance with the Texas Administrative Code</i></p> <p>Preliminary Objective:</p> <ul style="list-style-type: none"> To assess whether the data center services are performed in accordance to the requirements of the Texas Administrative Code, Chapters 202 and 215. 	750
-	<p><i>TEX-AN Vendor Management and Performance</i> **</p> <p>Preliminary Objective:</p> <ul style="list-style-type: none"> To assess whether the TEX-AN NG vendor(s) is being properly managed and performing in accordance to established service level agreements. 	750
	Assurance Audits – Tier 2 *	

Audit Project #	Audit Project Name/ Preliminary Objective(s)	Budgeted Hours*
-	<i>Vendor Sales Reporting for Non-USAS Customers</i> Preliminary Objective: <ul style="list-style-type: none"> To assist the Chief Procurement Office with developing a risk-based methodology for enhanced monitoring and oversight of vendors sales reporting. 	-
-	<i>Hybrid Cloud Services Billing</i> Preliminary Objective: <ul style="list-style-type: none"> To assess whether the management and accounting methods over the hybrid cloud services billing process are adequate and followed. 	-
18-200	Consulting and Non-Audit Services	
-	External Audit Coordination	200
-	Management Advisory Project (MAP)	80
-	Workgroups/ Governance Boards	100
-	Reserved for DIR Board and Executive Leadership Projects	275
18-300	Required Projects	
-	Follow-up on Audit Recommendations	350
-	Fiscal Year 2019 Internal Audit Risk Assessment/ Annual Plan	350
-	Fiscal Year 2018 Internal Audit Annual Report	40
-	Fiscal Year 2018 Internal Audit Annual Assessment	40
18-400	Special Projects	
-	External Assessment (Peer Review)	40
-	Risk Assessment Process Optimization	100

* Budgeted hours allocated to the projects included in the plan are based on the total available hours calculated for three approved full time equivalent employees (FTEs). All auditable activities identified as high-risk activities during the risk assessment process were included as assurance audits in Tier 1 or Tier 2 of the Fiscal Year 2018 Internal Audit Annual Plan, based on the agency’s risk appetite. However, due to limited resources no budgeted hours were allocated to conduct Tier 2 assurance audits. Tier 2 audits will be conducted by DIR Internal Audit if efficiencies are gained during the annual audit process. Otherwise, the residual risk will be re-assessed during the fiscal year 2019 Internal Audit Risk Assessment.

** Components of this assurance audit may include contract management activities.

The following table depicts additional auditable activities identified as high-risk that were not included in the Fiscal Year 2018 Internal Audit Annual Plan, including a brief description of such determination.

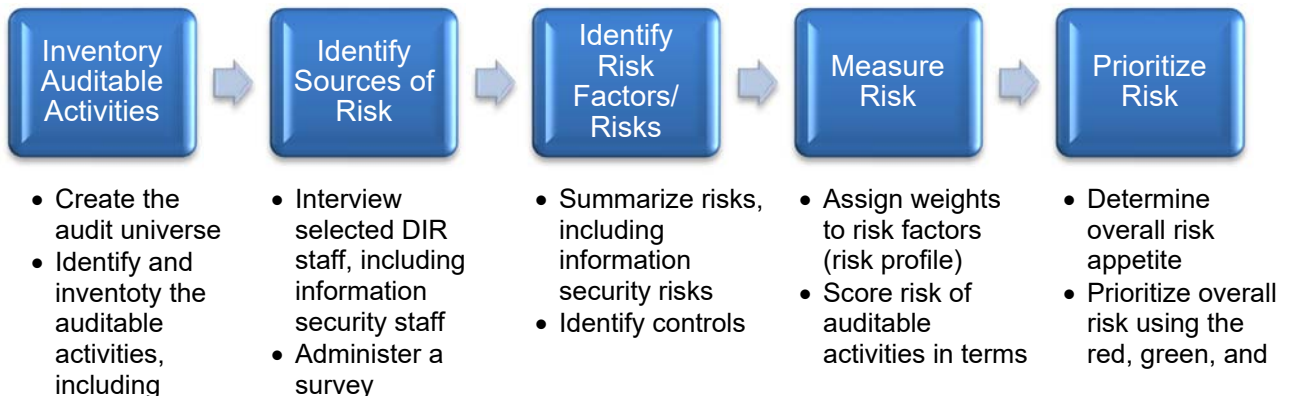
Auditable Activity	Description
1. Multi-Sourcing Integrator (MSI) Vendor Management and Performance	This auditable activity is undergoing a major re-procurement. The risk of this activity will be revisited after the new contract is executed and operations have reached a consistent degree of stability.
2. Texas.Gov Planning and Governance	This auditable activity is undergoing a major re-procurement. The risk of this activity will be revisited after the new contract is executed and operations have reached a consistent degree of stability.
3. Data Center Services (DCS) Vendor Management and Performance	This auditable activity is undergoing an assurance audit (#17-101: DCS Vendor Management and Performance) which provides partial audit coverage.

We are not aware that any of the audit projects included in the annual plan address benefit proportionality, expenditure transfers, capital budget controls, or any other limitation or restriction in the General Appropriations Act (GAA).

The Fiscal Year 2018 Internal Audit Annual Plan will be modified to accommodate any changes in risk that require modification of the plan. If needed, the revised plan will be submitted to the DIR Board for approval and a copy will be submitted to the oversight agencies, as required.

Risk Assessment Process

DIR Internal Audit implements a risk assessment process consisting of a hybrid methodology that uses specific risks, common risk factors, and risk categories aligned to the agency’s auditable activities and risk appetite.



- | | | | | |
|--|---|---|--|---------------------|
| information systems
• Organize the auditable activities | • Review relevant documentation, including information security
• Consider audit team knowledge/judgment
• Identify business objectives | • Select, define, and categorize the risk factors | of likelihood and impact
• Prioritize risk
• Determine overall risk scores | yellow color system |
|--|---|---|--|---------------------|

The following table depicts the risk categories and risk factors selected to assess, based on likelihood and impact, each auditable activity included in the risk assessment used to develop the annual plan.

Risk Category	Definition
Strategic	The possibility of an event occurring that will enhance or threaten the agency's prosperity and existence in the long term. <ul style="list-style-type: none"> • Negative Publicity/ Loss of Credibility • Poor Outcome to Customers
Operational	The possibility of an event occurring that will influence the ability of the agency to achieve its objectives through the transformation of inputs into outputs. <ul style="list-style-type: none"> • Lack of Adequate Resources • Lack of Operational Stability • Significant Dependence on Strategic Vendors and/or Contractors • Contractor Inadequacy

In addition, a review of the audit coverage (<= 3 years) for each auditable activity was conducted to assist in determining the overall risk. Consideration of information technology risks was integrated into the risk assessment process and addressed in terms of the functionality, confidentiality, integrity, availability, and reliability of the data created, processed, and stored in the agency's information systems.

The DIR risk-based audit plan was aligned to the agency's goals and risk appetite, and included input from the DIR Board and Executive Leadership Team (ELT). The DIR Board and ELT understand their responsibilities regarding risk and the importance of these risks exposures to the agency's governance, operations, and information technology.

VI. External Audit Services Procured in Fiscal Year 2017

The following external audit services were procured and ongoing in Fiscal Year 2017:

Financial Audit

- Texas.Gov Financial Audit for calendar year 2016

Assurance Audit

- Network Security Operations

VII. Reporting Suspected Fraud and Abuse

Actions taken by DIR to comply with the fraud requirements of:

[Section 7.09, page IX-38, the General Appropriations Act \(GAA\) – 85th Texas Legislature²](#)

- DIR included at the footer of its website home page a link to the State Auditor's Office (SAO) website for fraud reporting that includes the SAO fraud hotline information on how to report suspected fraud, waste, or abuse. The "SAO Fraud Reporting" link is in the DIR Home Page located at <http://dir.texas.gov/>.
- **DIR Ethics Policy Chapter 4. Policy Prohibiting Fraud, Waste, Theft, and Abuse** describes DIR's commitment to prevent fraud, waste, theft, and abuse by its employees and any consultant, vendor, contractor, other government entity or person in dealings with the agency or the State of Texas. In addition, the policy includes statements related to:
 - Security of Information Resources.
 - Fraud awareness training.
 - Responsibility to report suspected fraud, waste, theft, and abuse.

Each employee is required to report any suspected fraud, theft, waste or abuse to the agency. An employee may make a report to his or her supervisor, to an Ethics Officer or to the Internal Auditor. Fraud boxes and fraud reporting posters will be posted at conspicuous locations throughout

² GAA Section 7.09. Fraud Reporting – a state agency appropriated funds by this Act, shall use appropriated funds to assist with the detection and reporting of fraud involving state funds by 1) providing information on the home page of the entity's website on how to report suspected fraud, waste, and abuse involving state resources directly to the State Auditor's Office (SAO). This shall include, at a minimum, the SAO fraud hotline information and a link to the SAO website for fraud reporting; and 2) including in the agency's policies information on how to report suspected fraud involving state funds to the SAO.

the agency. Employees can report suspected fraud involving state funds to the State Auditor's Office (SAO) by calling (800) TX-AUDIT (892-8348) or by making a report online at <https://sao.fraud.texas.gov/ReportFraud/>. The agency will not retaliate against any individual for making a good faith report of suspected fraud, waste, theft or abuse. Any employee who believes he or she has suffered retaliation should immediately contact an Ethics Officer.

- Role of the Ethics Officer.
- Investigation of allegations of fraud, waste, theft, and abuse.
- Prohibited acts.
- Authority.

This policy is for all DIR employees, consultants, vendors, and contractors and establishes minimal requirements that are not all-inclusive. The absence of a specific rule covering any act discrediting an employee or the agency does not mean that the act is permissible or would not call for disciplinary action, including immediate termination, when considered necessary.

- DIR Internal Audit carries the responsibility of reporting any issue of fraud to the SAO, as required.

[Texas Government Code \(TGC\), Section 321.022, Coordination of Investigations³:](#)

The DIR Executive Director or designee reports money lost, misappropriations, misuse, and any other fraudulent or unlawful conduct to the SAO, as required, when reasonable cause is believed that fraudulent or unlawful conduct may or has occurred in relation to DIR's operations.

³ Texas Government Code, Section 321.022. Coordination of Investigations – states if the administrative head of a department or entity that is subject to audit by the SAO has reasonable cause to believe that money received from the state by the department or entity or by a client or contractor of the department or entity may have been lost, misappropriated, or misused, or that other fraudulent or unlawful conduct has occurred in relation to the operation of the department or entity, the administrative head shall report the reason and basis for the belief to the SAO.

Appendix A: Report Distribution

Internal Report Distribution

Department of Information Resources (DIR) Board

DIR Executive Director

External Report Distribution

Texas Office of the Governor

Texas Legislative Budget Board

Texas State Auditor's Office

Texas Sunset Advisory Commission

Department of Information Resources
Internal Audit

Fiscal Year 2017 Internal Audit Annual Report

APPROVAL:



Lissette Nadal

DIR Internal Audit Director

1/22/18

Date



Ben Gatzke

DIR Board Chair/ Finance and Audit Subcommittee Chair

Jan 25, 2018

Date