

DIR Annual Internal Audit Report FY2011

November 2011

Table of Contents

Internal Audit Plan for Fiscal Year 2011	2
Introduction	3
Mission.....	3
Internal Audit Charter	3
Audit Staff/Resources Available.....	3
Planned Internal Audit Activities.....	4
Risk Assessment Process for FY2011.....	4
External Quality Assurance Review (Peer Review)	4
List of Audits Completed.....	5
List of Consulting Engagements and Non-audit Services Completed.....	11
Organizational Charts.....	12
Report on Other Internal Audit Activities	13
Internal Audit Plan for Fiscal Year 2012.....	14
External Audit Services Procured in Fiscal Year 2011	15
Reporting Suspected Fraud and Abuse	18

Internal Audit Plan for Fiscal Year 2011

Department of Information Resources Internal Audit Division FY 2011 Internal Audit Plan

Audit Projects

Audit Projects:	Projected Hours
Telecom Invoicing Process	260
Data Center Invoicing Process	260
ICT Review of Vendor Reporting and Fee Process	140
ICT Contract and Service Process	160
Management of DIR Enterprise Contracts	160
Finance and Accounting Reconciliation Review	160
Monitoring Projects:	
Data Center Activity	80
Texan Next Generation Contract	80
Audits from Outside Auditors	80
Follow-up on Past IA Audit Recommendations	32
Follow-up on SAO Recommendations	40
Board & ED Special Projects	
Reserved For Board Projects	80
IA Administration	80
Other projects (required by law and auditing standards):	
Continuing Professional Education	40
Annual Internal Audit Report	60
Annual Risk Assessment Process for 2011	40
Annual Risk Assessment Process for 2012	80
Total Hours	1832

Introduction

The purpose and objective of the Internal Audit Plan is to outline audits and other activities the Internal Audit function will conduct during fiscal year 2011 and to allocate audit resources to key activities identified within DIR using risk assessment techniques and methodology. The audit plan satisfies responsibilities established by Government Code, Chapter 2102, and applicable auditing standards.

The Audit Plan is flexible to consider risks and changes in conditions on an ongoing and as needed basis.

Mission

The Internal Audit function is an independent, objective assurance and consulting activity designed to add value and improve the organization's operations. Internal Audit assists the Board, management, and staff to achieve its vision, mission, values, and goals. In so doing, it seeks to help the organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes. In addition to providing auditing services, Internal Audit coordinates with external auditors and provides consulting and advisory services as appropriate.

Internal Audit conducts its activities in compliance with the DIR Internal Audit Charter, the Texas Internal Auditing Act, and applicable Internal Audit Standards as outlined in the Internal Audit Charter.

Internal Audit Charter

The Internal Audit Charter provides authorization to the Internal Audit function for full, free, unrestricted access to all DIR activities, records, property, and personnel relevant to the subject under review. Internal Audit will exercise due diligence in the safeguarding and use of these resources.

Audit Staff/Resources Available

In February of FY2011, DIR's internal audit increase to two fulltime equivalent employees. The Internal Auditor is the Chief Audit Executive and reports directly to the Board and administratively to the Executive Director. There were 1832 scheduled hours calculated for audits, follow up reviews, external audit coordination, and special projects including consulting and advisory services for FY 2011.

Planned Internal Audit Activities

The Texas Internal Auditing Act requires state agencies to conduct a program of internal auditing that includes an annual audit plan that is prepared using risk assessment techniques and that identifies the individual audits to be conducted during the year. Additionally, the program should include periodic audits of the agency's major systems and controls, including:

- (1) accounting systems and controls;
- (2) administrative systems and controls; and
- (3) electronic data processing systems and controls.

Scopes of audits can be financial, compliance, economy and efficiency, effectiveness or may be investigative in nature.

The Internal Audit Plan of Activities includes results from the risk assessment and input from Division Directors and the Executive Director. Hours budgeted for projects are best estimates. Many unforeseeable factors can increase or decrease total hours allotted to a project.

Due to limited resource hours, Internal Audit cannot address, review, or monitor every risk. It is important that the Executive Director and the Board understand the limitations of the audit coverage and the attendant risk for areas not audited.

Risk Assessment Process for FY2011

Auditable units are key activities and processes performed by the agency and were determined by reviewing the agency's Strategic Plan, the agency's FY2011 Budget, organization charts, applicable governing statutes, and interviews.

External Quality Assurance Review (Peer Review)

DIR's Internal Audit function is due for an External Quality Assurance or Peer Review in 2 years. According to the Institute of Internal Auditors (IIA), an external assessment should be conducted at least once every five years by a qualified, independent reviewer or review team from outside the organization.

According to the Government Auditing Standards (GAS), Audit organizations should have an external quality control review completed within three years from the date the first audit begins in accordance with these standards. After the issuance of the review, a subsequent external quality control review should occur once every three years.

DIR's Annual Internal Audit Report

List of Audits Completed

Report No.	Report Date	Name of Report	High-level Audit Objective(s)	Observations/Findings and Recommendations	Current Status (Fully Implemented, Substantially Implemented, Incomplete/Ongoing, or Not Implemented)	Fiscal Impact/ Other Impact
10-301	10/2010	Procurement and Management Process for Staffing Service Contractors	The objective of the audit was to determine if written policies and procedures exist, if DIR follows purchasing guidelines, and if DIR monitors the contract staffing services process to ensure it achieves its goals and objectives and meets the needs of the agency.	<p>The agency does not have written policies and procedures for overseeing its contract staffing services. Thus, the approach used by the agency can be inconsistent, inefficient, costly and inappropriate. Originally, there seems to have been an understanding of how to procure staffing services. Over time, there has been a misunderstanding of the original directive due to not documenting the policies and procedures. Well-written and followed policies and procedures ensure consistency, and are essential for accountability, proper expenditures, efficiency, and effectiveness.</p> <p>DIR should develop and implement written policies and procedures that establish controls for the procurement and administration of contracted staffing services.</p>	Fully Implemented	Ensures that objectives of the program are achieved.
10-301				<p>DIR augments its staff using staffing service contractors in order to meet statutory obligations and maintain services. Managers using the best value method do not always fully document the justification and do not document that other options have been considered and fully explored. Incomplete written justification may not support the decision to contract out for staff augmentation, and there are no formal guidelines on documenting justification to hire staffing services contractors.</p> <p>DIR should thoroughly document the justification for selecting a vendor solution, and the individual contractor.</p>	Fully Implemented	Management of the program is improved.

10-301				<p>DIR has no standards for contractors to report time. Depending on the division, the contractor uses an in-house time card or the vendor's own time card. Due to this, time cards are not consistent. Without a standardized time card format, it may be harder to discover discrepancies, patterns, or obtain other valuable information. Since standards do not exist, each division determines how to best report contractor hours for payment of work performed. Standards for recording contractor work hours will allow the agency to manage and review contractors' time, cost, and scope of work</p> <p>DIR should standardize contractor timesheets for consistent use throughout the agency and look at the feasibility of acquiring a computerized timekeeping system.</p>	Ongoing	Implements controls over processes.
10-301				<p>There is no evidence in the purchasing documents reviewed indicating that anyone requested or negotiated a reduced hourly rate. Reports indicated that the majority of the time DIR pays at the ICT agreed upon rate. DIR employees should negotiate the best rate possible.</p> <p>When procuring staffing services, DIR should determine if they can negotiate a lower rate from the vendor than the ICT agreed rate.</p>	Fully Implemented	Increases the use of negotiation tools available to the program.
10-301				<p>The agency selected one vendor to supply the majority of contractors needed for the Health and Human Services Commission's Integrated Eligibility and Enrollment Program. While this may be justified, there can be a perception that one contractor or vendor is being favored. IA also found there was not effective oversight in managing these contractors. Not having the appropriate oversight could result in the misuse and abuse of State resources. Also, there needs to be a distinction regarding the distinct roles and responsibilities of contractors and DIR employees, including responsibilities relating to contract management.</p> <p>DIR should develop policies for the oversight of augmented staffing services that ensures consistent monitoring of the work and the calculation of time.</p>	Fully Implemented	Increases controls over State resources.

11-101	August 2011	Contract Establishment and Monitoring Process	The objective of the audit was to determine if written policies and procedures are documented, current, followed, and in compliance with state guidelines. Additionally, the appropriateness of the methodology used for establishing a contract and the effectiveness of the vendor selection during the contract negotiation process were examined. The audits also examined the reasonableness of the contract negotiation process with selected vendors and looked at vendor sales to determine if they were monitored and accurately reported.	<p>The Detail Fee Report, prepared by the Contract Performance Data Analytics Team, does not present the same amounts as the actual sales reports submitted by vendors. Actual dollar amounts reported by vendors on their sales reports should equal the Detail Fee Reports used by ITC Division Management and anyone who asks for a copy. The Data Analytics Team has formatted the Detail Fee Report to round sales dollar amounts reported by vendors.</p> <p>ICT Division Management should reformat sales reports to show actual amounts reported by vendors and not the rounded totals.</p>	Fully Implemented	Improves management information for decision making.
11-101				<p>ICT Division Management created more up-to-date procedures in March 2011; however, procedures were incomplete in that there was no section for the Monthly Administrative Fee Reconciliation procedure. The draft purpose of this procedure was “to ensure that the GoDirect Administrative Fees due from vendors are accounted.” ICT Division Management did not update the program procedures between May 2006 and March 2011.</p> <p>ICT Division Management should keep procedures current and ensure that all procedures are complete and approved by management.</p>	Incomplete/Ongoing	Improves consistency of the program.
11-101				<p>Internal Audit examined the CDI Payment Summary Report used by ITC Division Management. IA determined that in November 2010, 44.14% of administrative fee payments received by DIR had no or substandard documentation attached to assist with identifying which contract is associated with a payment.</p> <p>ICT Division Management should require vendors to submit a remittance summary with the sales report.</p>	Substantially Complete	Improves fiscal accountability over payments.

11-101				<p>Some vendors do not pay the administrative fees due to DIR. Some contract files do not show documentation indicating that Contract Managers ask vendors to pay delinquent fees owed to DIR. There is no evidence that Contract Managers take a proactive approach to ask vendors on a monthly basis to report and pay the correct administrative fees. ITC Division Management has explained that Contract Managers do not contact vendors until the contract is up for renewal amendment.</p> <p>ICT Division Management should require that Contract Managers follow procedures and contact vendors monthly if the administrative fee is not timely submitted. Management should establish an effective way for Contract Managers to monitor vendor performance.</p>	Fully Implemented	Ensures DIR receives all funds due from contract sales.
11-101				<p>Inconsistent language may cause disputes with vendors over audit coverage. In addition, by altering the audit clause uniquely for each vendor, the preparation and conduction of audits will become inefficient and lengthy, requiring use of additional resources. IA has the right to audit all aspects of DIR operations. The wording of the contract may cause vendors to challenge IA's right to audit.</p> <p>DIR should require standard wording in the <i>Right to Audit</i> clause in all agency contracts and not allow vendors to negotiate and change wording.</p>	Fully Implemented	Ensures DIR's right to audit clause is incorporated into contracts to increase effectiveness.
11-101				<p>ICT Contract Managers are not adhering to the procedures requiring them to contact delinquent or non-reporting vendors and obtain past due reports even though they were aware of the past due vendors.</p> <p>ICT Division Management should enforce program procedures, establish standards for obtaining sales reports from delinquent and non-reporting vendors, ensure vendors submit monthly sales reports to DIR, and require that all vendor communications be documented in the contract file and on Salesforce.com.</p>	Incomplete/Ongoing	Ensures DIR receives funds due from vendor sales.

11-101				<p>IA analyzed documentation in the contract files and on Salesforce.com for nine vendors who had not reported between eight and thirteen times. Even though some of these vendors had been contacted by the Contract Manager to send in the delinquent reports, four of the nine vendors were still delinquent when their contracts were amended to extend the term.</p> <p>ICT Division Management should establish an effective contract monitoring process that ensures vendors who do not report activity are notified of their contractual obligations to report monthly even if they had no sales. In addition, contract monitoring should ensure that DIR is receiving all administrative fees due, and ensure that a contract is not renewed if the contract terms have not been met.</p>	Incomplete/Ongoing	DIR is assured that vendors are meeting their contractual obligations stated in the ICT Contracts.
11-101				<p>IA was informed that critical data analytics Oracle tables and Business Objects applications are stored on his personal computer. IA was also informed that if the manager left the agency, there would not be a backup person to handle the creation of management reports and thus information and institutional knowledge may be lost.</p> <p>ICT Division Management should follow existing procedures for obtaining approval for application development from the information resources manager and cross-train employees to create and run management reports.</p>	Incomplete/Ongoing	Ensures that critical data is not lost and management reports are available.
11-101				<p>Contract Performance Managers are assigned to amend or renew the same contracts that they monitor for performance. This assignment of responsibilities is a concentration of duties by having the same person who negotiates the contract also monitor for performance. This concentration of duties creates a risk to the agency since errors or omissions may not be discovered in a timely manner.</p> <p>ICT Division Management should separate the duties of employees so that there is a clear line of independence between the establishment and the performance monitoring of ICT contracts. Also, the ICT Division Director should assign contract amendments and renewals duties only to the Contract Establishment Managers.</p>	Incomplete/Ongoing	Independence is maintained between contract monitoring and contract establishment.

Definitions of implementation status are as follows:

- Fully Implemented: Successful development and use of a process, system, or policy to implement a prior recommendation.
- Substantially Implemented: Successful development but inconsistent use of a process, system, or policy to implement a prior recommendation.
- Incomplete/Ongoing: Ongoing development of a process, system, or policy to address a prior recommendation.
- Not Implemented: Lack of a formal process, system, or policy to address a prior recommendation

List of Consulting Engagements and Non-audit Services Completed

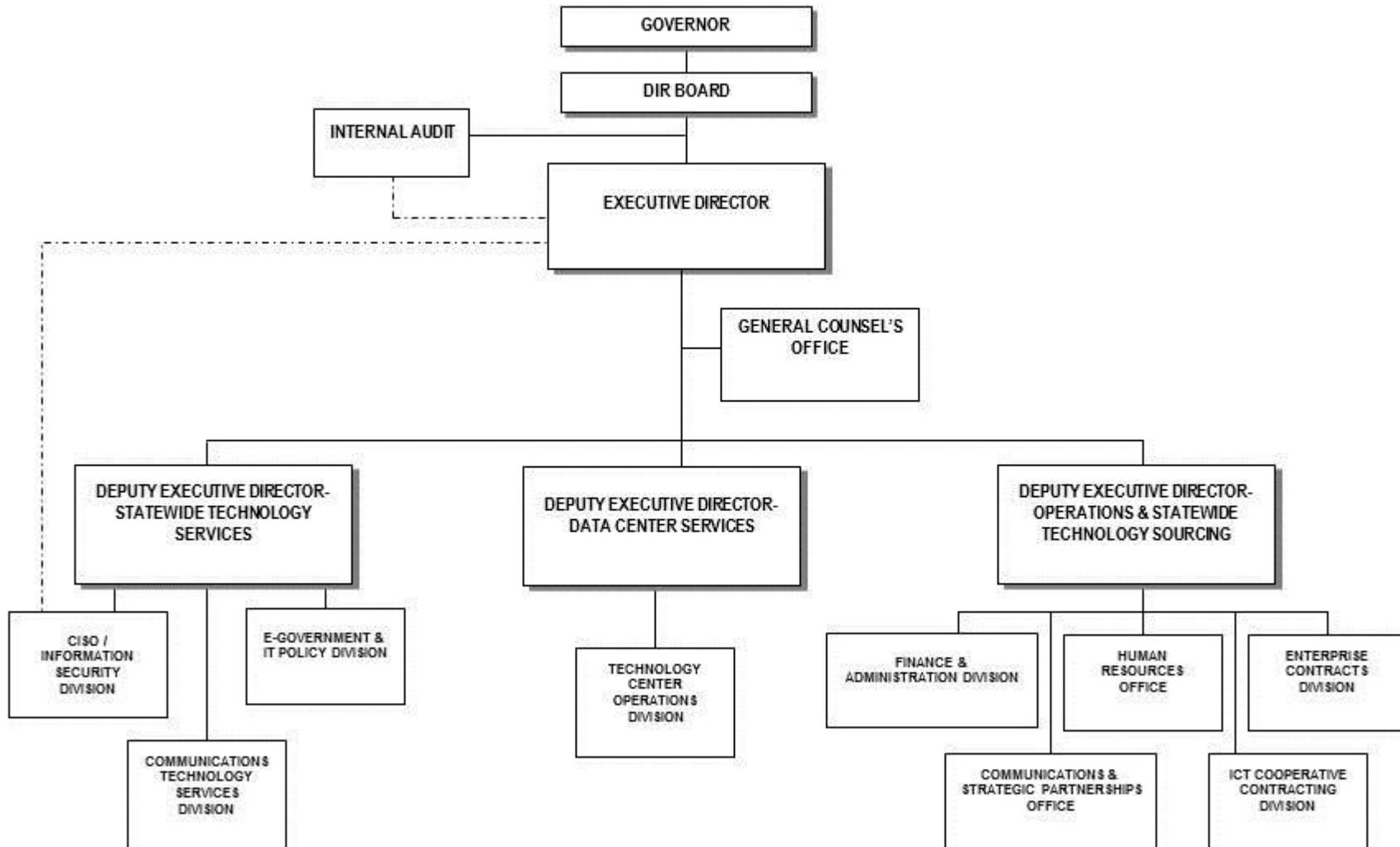
Audit No.	Date	Name	High-level Consulting Engagement/Non-audit Service Objective(s)	Observations/ Results and Recommendations	Current Status (Fully Implemented, Substantially Implemented, Incomplete/Ongoing, or Not Implemented) with Brief Description If Not Yet Implemented ²	Fiscal Impact/ Other Impact
	1/2011	Data Center Services Program Contract-to-Date Cost Assessment Report.	Request to review and analyze the report to determine whether the methodology used is sound.	Determined that the methodology is sound.	Fully Implemented	N/A
	3/2011	Technology Policy Management	Agency wide initiative to review DIR statutes, rules, policies, standards, guidelines, and procedures. Internal Audit was asked to review the methodology and strategy to implement the points in the report.	Management established a process to improve documentation at DIR.	Ongoing	N/A
	3/2011 to 10/2011	Assist ICT Division during State Auditor audit of the program.	Coordinated communication between the division and the SAO. Advised management during the process.	SAO report was issued.	Fully Implemented	N/A
	9/2010 to 8/2011	Advised DIR management on risk mitigation strategies.	Objective is to assist management.	N/A	Ongoing	N/A

- Fully Implemented: Successful development and use of a process, system, or policy to implement a prior recommendation.
- Substantially Implemented: Successful development but inconsistent use of a process, system, or policy to implement a prior recommendation.
- Incomplete/Ongoing: Ongoing development of a process, system, or policy to address a prior recommendation.
- Not Implemented: Lack of a formal process, system, or policy to address a prior recommendation.

TEXAS DEPARTMENT OF INFORMATION RESOURCES (DIR)

Organization Chart

June 2011



Report on Other Internal Audit Activities

Activity	Impact
DIR Internal Audit acquired and has implemented an automated audit software to assist in the performance of audits.	Efficient use of resources with enhanced data storage.
Internal Audit department participated in continuing education activities as required by the Standards.	Internal Audit employs two certified auditors who each require 40 hours of continuing education annually.
Internal Audit was the intergovernmental liaison between other State agencies' audit functions.	Improved the public perception of DIR.

Internal Audit Plan for Fiscal Year 2012

Audit Projects		Hours
11-100	In Process FY2011 Audits to complete	
11-102	-Data Center Invoice	120
11-103	-Management of DIR Enterprise Contracts	80
11-101	-Telecom Invoicing Process	270
11-104	-Finance and Accounting Reconciliation Review	80
12-100	FY2012 Audits	
12-101	Technology Center Operations – Transformation	300
12-102	E-Government & IT Policy – Statewide Project Delivery	200
12-103	Technology Center Operations – Server Tower	300
12-104	CISO/Information Security	360
12-200	FY2012 Division Management Requested Audits	
12-201	E-Government & IT Policy – Texas.Gov	320
12-202	E-Government & IT Policy – Technical Service Delivery	180
12-203	E-Government & IT Policy – Policy and Research	140
12-300	Monitoring Projects:	
12-301	Data Center Activity	80
12-302	Texan Next Generation Contract	80
12-303	Audits from Outside Auditors	300
12-304	Follow-up on Past IA Audit Recommendations	20
12-305	Follow-up on SAO Recommendations	20
12-400	Board & ED Special Projects	
12-401	Reserved For Board Projects	100
12-402	IA Administration	100
12-300	AutoAudit software SQL implementation:	
12-306	Data for Sunset Commission recommendations.	40
12-307	Data for State Auditor’s Office recommendations.	40
12-308	Data for SAS 70 & SSAE 16 recommendations.	40
12-500	Other projects (required by law and auditing standards):	
12-501	Continuing Professional Education	80
12-502	Annual Internal Audit Report	20
12-503	Annual Risk Assessment Process for 2013	40
Total		3310
Hours		

External Audit Services Procured in Fiscal Year 2011

DIR Request for External Audit Services			
Auditor	DIR Area	Audit Description	Audit Begin Date
KPMG	Data Center	SAS 70 Audit. Contractual requirement for SAS 70.	June 2011
Clifton Gunderson LLP	E-Government (Texas.gov)	Texas Online Financial Statements Audit	March 2011
Request for Information from Outside Auditors			
Auditor	DIR Area	Audit Description	Audit Begin Date
HHSC 2010 Internal Revenue Service Onsite Safeguard Review	Data Center	The Texas Health and Human Services Commission on-site Internal Revenue Service (IRS) Safeguards review	September 2010
HHSC -Food and Nutrition Services on-site assessment of the TxEBT System as deployed at the Austin Data Center (ADC) and the San Angelo Data Center (SDC).	Data Center	FNS will review the TxEBT System infrastructure (configurations, designs, and performance metrics) to gain an understanding of the system's environments. FNS will require on-site visits to the ADC and SDC to confirm the security and infrastructure requirements are in place as approved and documented. Further, FNS will evaluate system to determine if the current infrastructure will support the projected growth requirements of the Texas SNAP EBT System.	October 2010
HHSC 2011 Internal Revenue Service Onsite Safeguard Review – San Angelo Data Center	Data Center	The Texas Health and Human Services Commission on-site Internal Revenue Service (IRS) Safeguards review in February 2011 of the San Angelo Data Center.	January 2011

<p>Health and Human Services Commission (HHSC) Internal Audit of Enterprise Information Security</p>	<p>Data Center</p>	<ul style="list-style-type: none"> • Assess the effectiveness of current controls over the security of confidential data collected and maintained by: <ul style="list-style-type: none"> o HHSC agencies and o Responsible contractors and business partners working on behalf of HHSC agencies. • Evaluate compliance with federal, state, and HHSC Enterprise data protection requirements. • Present comparative information, as reported by management, on: <ul style="list-style-type: none"> o HHSC agency implementation of the key components of a comprehensive information security program. o The extent to which information security efforts are coordinated and required resources are leveraged across the enterprise. o Planned information security initiatives and improvements to existing controls 	<p>April 2011</p>
<p>Texas Health and Human Services Commission on-site Internal Revenue Service (IRS) Safeguards review on April 27, 2011 for the Winters Data Center (WDC)</p>	<p>Data Center</p>	<p>Overview of the IRS safeguards implemented at the WDC-IRS Safeguard Review Internal Inspections Report</p>	<p>April 2011</p>
<p>Clifton Gunderson LLP 2011 SSAE 16 Audit for the Electronic Benefits Transfer System, Health and Human Services Commission</p>	<p>Data Center</p>	<p>The SSAE 16 Type II audit for the Electronic Benefit Transfer system of the State of Texas will address the operational effectiveness of the controls from September 1, 2010 through August 31, 2011 for data center operations for the Texas EBT system which includes, but is not limited to the following:</p> <ul style="list-style-type: none"> 24x7 operator support Data center security Batch job processing Network management and security EBT transactions monitoring Third-party processors support EBT software products support Database maintenance and administration Project, change, and quality management for system enhancements and new features 	<p>April 2011</p>
<p>Audit by the Health and Human Services Commission, Internal Audit Division</p>	<p>Data Center</p>	<p>Human Resources (HR) information systems included in the scope of this audit are:</p> <ul style="list-style-type: none"> • Health and Human Services (HHS) Administrative System Human Resources Management System (HHSAS HRMS) application and database, • AccessHR applications and databases, • Network environments that support HR information systems, and • HHSAS HRMS and AccessHR interfaces. 	<p>June 2011</p>

<p>DIR IT audit of the LAN infrastructure in place at the Austin Data Center and the San Angelo Data Center.</p>	<p>Data Center</p>	<p>The scope of the audit is limited to the LAN infrastructure at the two State data centers, including the core layer, distribution layer, access layer, backup and storage. The audit will include inspection of connections between devices (host to switch and among switches, routers, appliances, etc.) as well as an evaluation of installed network management devices for redundancy, load-balancing/content management, security appliances (firewalls, IDS, access controls) and software, over-subscription, reporting capability, disaster recovery and data replication, and other criteria that are described in the network standards documentation provided by DIR and/or by current industry standards and best practices for LAN infrastructure deployment and operation.</p>	<p>June 2011</p>
<p>IBM engaged KPMG –SSAE-16 audit to be conducted in accordance with Section 9.9.(g)(i) of the Agreement.</p>	<p>Data Center</p>	<ol style="list-style-type: none"> 1. IBM will engage an independent public accounting firm to conduct the SSAE-16 audit of the San Angelo and Austin Data Centers. 2. The audit will begin no later than July 2011 and will cover the period of September 1, 2010 through September 30, 2011. 3. The audit will encompass the standard data center processes around the following controls: <ul style="list-style-type: none"> • Physical access, with focus on background checks where required and addition and removal of access • Backup and recovery • Job scheduling • Software change control • Logical security with focus on ID administration, access addition and timely removal, and security patching 4. Any audit activity concerning Co-location Services will be limited to physical access only. 	<p>July 2011</p>
<p>TWC review of documentation (policies, procedures, and network diagrams) and guided examination of the data / physical environments apportioned to the Texas Workforce Commission mainframe(s) and mid-range servers at the Austin Data Center.</p>	<p>Data Center</p>	<p>This effort is focused upon acquiring certification & accreditation under the Federal Information Security Management Act (FISMA) and OMB Circular A-130 using the following references:</p> <ul style="list-style-type: none"> • NIST SP 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems • NIST SP 800-53 Recommended Security Controls for Federal Information Systems and Organizations <p>Areas of primary interest are:</p> <ul style="list-style-type: none"> • Security controls provided by IBM surrounding the TWC LPARs; and • Closely coupled mid-range servers including their logical and physical mapping for connectivity through the Austin Data Center back to Texas Workforce Commission. 	<p>July 2011</p>
<p>The Texas Department of Information Resources - “Payment Card Industry (PCI) Certification Review” for Texas.gov. The recertification-conducted by ATsec Information Security in collaboration with the quarterly wireless scans performed by Clifton Gunderson.</p>	<p>Data Center</p>	<p>The certification review will verify Texas.gov compliance with the PCI Data Security Standard, whereby service providers may be required to validate and conduct a network security scan on a regular basis as defined by the PCI Security Standards Council and/or complete other templates and protocols for certification.</p>	<p>August 2011</p>

Reporting Suspected Fraud and Abuse

Actions taken to implement the requirements of:

- **Fraud Reporting.** Article IX, Section 17.05, the General Appropriations Act.
- **Reporting Requirements.** Article XII, Section 5(c), the General Appropriations Act (81st Legislature).
- Texas Government Code, Section 321.022.

No suspected fraud and abuse to report.