

Background:

The Audit Committee has reviewed the enclosed documents at the Committee meeting October 18th and approved submission on behalf of the Council to the State Auditor’s Office, Governor’s Office of Budget, Planning and Policy, Legislative Budget Board and Sunset Advisory Commission. These reports are required to be submitted by November 1st of each year. TCDD Policies allow the Audit Committee to approve submittal on behalf of the Council subject to review by the Council. Should the Council choose to make revisions; a revised report can be submitted.

The reports include:

- TCDD FY 2010 Annual Internal Audit Report
- TCDD Internal Audit Report #2010-1: TAC 202
- TCDD Internal Audit Plan for FY 2011

This item was deferred during the November Council meeting due to time constraints.

Council Meeting

Agenda Item 8.

Expected Action:

The Council will review, revise as appropriate, and approve the TCDD Audit Reports.



TEXAS COUNCIL FOR DEVELOPMENTAL DISABILITIES

ANNUAL INTERNAL AUDIT REPORT

Fiscal Year 2010

Presented to
TCDD Audit Committee
October 18, 2010

Prepared by:
Rupert & Associates, PC
Certified Public Accountants
Austin, Texas

Texas Council for Developmental Disabilities (TCDD)
ANNUAL INTERNAL AUDIT REPORT – FY-2010

Table of Contents

I.	Internal Audit Plan for Fiscal Year 2010.....	1
II.	External Quality Assurance Review	1
III.	List of Audits Completed.....	2
IV.	List of Consulting Engagements and Non-Audit Services Completed.....	3
V.	Organizational Chart.....	4
VI.	Report on Other Internal Audit Activities	5
VII.	Internal Audit Plan for Fiscal Year 2011	5
VIII.	External Audit Services	6
IX.	Reporting Suspected Fraud and Abuse	6
	Report Distribution Page.....	7

Texas Council for Developmental Disabilities (TCDD)
ANNUAL INTERNAL AUDIT REPORT – FY-2010

I. Internal Audit Plan for Fiscal Year 2010

The internal audit plan for TCDD for fiscal year 2010 was based on risks identified in the FY10 risk assessment update. The plan identified the following objectives as the main areas of focus for internal audit.

1. Information Technology: An assessment of compliance with TAC 202, Information Security Standards, which will also comply with the requirement for a periodic audit of TCDD's major systems and controls, including safeguarding of assets and data. As needed, consult, advise, and monitor the development and refinement of the grantee reporting database (DD Suite).
2. Follow up on prior year audit recommendations.

II. External Quality Assurance Review (QAR)

An external quality assurance review was performed in April of 2009 by David J. MacCabe, CIA, CGAP, MPA, covering TCDD internal audit activities performed by the internal audit contractor (Rupert & Associates) during the period July 2007 through June 2009. The contracted internal audit function at TCDD was found to fully comply with the Institute of Internal Auditors (IIA) *International Professional Practices Framework* including the *International Standards for the Professional Practice of Internal Auditing*, the *Definition of Internal Auditing*, and the *Code of Ethics*, the United States Government Accountability Office (GAO) *Government Auditing Standards*, and the Texas Internal Auditing Act (*Texas Government Code*, Chapter 2102). Opportunities for improvement recommended by the reviewer include:

1. Consider updating the Audit Committee Charter
2. Plan future audit projects to include evaluation of organizational governance

Recommendations from the QAR have been implemented. The Audit Committee Charter was reviewed and updated in October of 2009 and will be reviewed annually and updated as needed. Future audit projects will include elements of organizational governance within other audit programs as appropriate.

III. List of Audits Completed

The table on the following page provides a list of audits completed during fiscal year 2010 with high-level objectives, summarized key audit observations and recommendations, including impact and implementation status of each.

Texas Council for Developmental Disabilities (TCDD)
ANNUAL INTERNAL AUDIT REPORT – FY-2010

III. List of Audits Completed Showing High-Level Objectives, Observations / Findings, Recommendations, and Status

Report #	Rpt Date	High-Level Audit Objective(s)	Rec #	Observations/Findings and Recommen	Current Status	Fiscal Impact / Other Impact	
2010-01	8/6/2010	Information Security Standards (TAC 202)					
	Objective A	Determine what the roles and responsibilities of TCDD and TEA are related to TAC 202 compliance requirements.	2010-1	Develop a written Business Recovery Plan for TCDD that will interface with TEA efforts for systems and business recovery in the event of an incident.	In Process: TCDD has adopted Operating Procedure 01-11 Business Continuity Planning that establishes procedures for TCDD business continuity planning in order to ensure the quick and effective recovery of mission-essential business functions in the event of a disaster or major business interruption that impairs the operations of the TCDD. In addition, TCDD IT functions are included in the TEA Business Continuity Plan version 1.0 dated January 2010. TCDD will review this matter further with TEA to determine if additional information is needed by TEA to restore TCDD IT functions should that be necessary. TCDD has recently developed and adopted an Emergency Backup Succession Plan to address organizational stability and leadership continuity of the Executive Director and key management staff.	Compliance with TAC 202 information security standards for state agencies.	
	Objective B	Determine if TCDD has adequate procedures in place to ensure that they meet their responsibilities as described in TEA's information security procedures.	2010-2	Agency policy calls for employees to sign an acknowledgement of appropriate usage policy at the time of hire. In addition to this initial acknowledgement, TCDD should encourage a reiteration of the risks of inappropriate technology usage.	Implemented: TEA currently offers security classes through their Office of Organizational Effectiveness. These classes are open to TCDD staff. TCDD staff receive emails regarding security class curriculum and schedules. TCDD staff is encouraged to sign up for these classes to raise security awareness and reinforce security usage. Appropriate use of technology is discussed periodically during TCDD staff meetings.	Raise awareness of information security risks among staff.	
	Objective C	Determine if TEA provides appropriate monitoring and oversight of TCDD information security control processes to meet the IT security standards.	2010-3	TCDD should work with the TEA ISO to identify the level of security support to be provided by TEA and the activities for which TCDD is responsible. The interagency MOU should be revisited to clearly define the responsibilities for these procedures, including IT security oversight	Implemented: TCDD believes the responsibilities of TEA and of TCDD related to IT services and security are clear and appropriate within the current MOU. The MOU defines the Information technology support provided for TCDD by TEA, including support through the Department of Information Resources and the state Data Center Service.	Operational efficiencies and compliance with state requirements.	

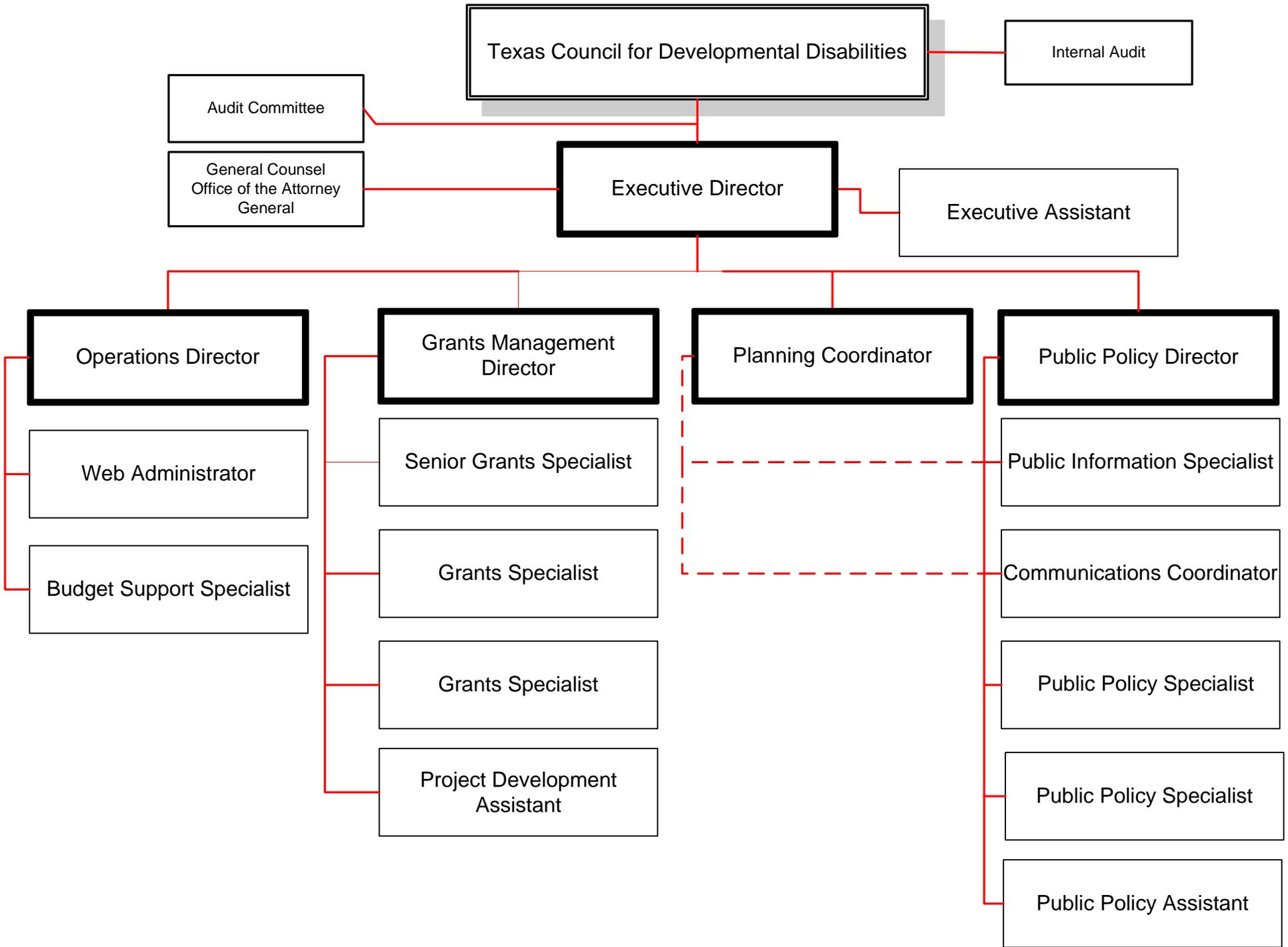
Texas Council for Developmental Disabilities (TCDD)
ANNUAL INTERNAL AUDIT REPORT – FY-2010

IV. List of Consulting Engagements and Non-audit Services Completed Showing High-Level Objectives, Observations/Results, Recommendations, and Status

There were no consulting engagements or non-audit services performed in FY10.

V. Organizational Chart

A current organizational chart is provided on the following page.



**Texas Council for Developmental Disabilities (TCDD)
ANNUAL INTERNAL AUDIT REPORT – FY-2010**

VI. Report on Other Internal Audit Activities

Activity	Impact
Annual Risk Assessment Update	Facilitated management in the review and update of their risk assessment, including fraud risk factors, and mitigating strategies.
Internal Audit Quality Assurance and Improvement Program (QAIP)	Professional standards checklists, working paper reviews and quality self-assessments are performed on all audits.
External Quality Assurance Reviews (QAR)	External Quality Assurance Reviews are performed on the internal audit function at TCDD in accordance with the Texas Internal Auditing Act.
State Agency Internal Audit Forum (SAIAF)	Participated in SAIAF to stay abreast of changes in standards and/or legislation that may impact internal audit's role in state agencies.
The Institute of Internal Auditors International Conference	Attend various internal audit training events, including the international conference in 2010, to stay abreast of changes in the professional standards.

VII. Internal Audit Plan for Fiscal Year 2011

Based on the updated risk assessment, the proposed internal audit focus for FY-2011 is:

3. Grantee Monitoring: Review and evaluate current grantee monitoring procedures and controls. As needed, consult, advise, and monitor the development and refinement of the grantee reporting database (DD Suite).
4. Follow up on prior year audit recommendations.

Alternative audit areas are proposed in the event that circumstances prevent the implementation of the planned audit, or if additional resources are available for more audit work. An alternative audit areas proposed is IT security over social media sites.

Texas Council for Developmental Disabilities (TCDD)
ANNUAL INTERNAL AUDIT REPORT – FY-2010

VIII. External Audit Services

External audit services procured in fiscal year 2010 consisted of the internal audit function and independent CPA services for performing desk reviews on grantee audit reports.

IX. Reporting Suspected Fraud and Abuse

Actions taken to implement the requirements of Article IX, Section 17.05, and Article XII, Section 5(c), the General Appropriations Act (81st Legislature) and Texas Government Code, Section 321.022) include the placement of a link on the TCDD website to connect users directly to the State Auditor's Office website page for reporting suspected fraud, waste, or abuse.

TCDD Policies also provide guidance for anyone wanting to report suspected fraud or abuse. Grantees are provided guidance on reporting fraud in the TCDD Grants Manual.

**Texas Council for Developmental Disabilities (TCDD)
ANNUAL INTERNAL AUDIT REPORT – FY-2010**

REPORT DISTRIBUTION PAGE

Texas Council for Developmental Disabilities, Audit Committee

Mary Durham, Chair
John Morris, Vice-Chair
Andrew Crim, Member
Marcia Dwyer, Member
Brenda Coleman-Beattie, Council Chair

Texas Council for Developmental Disabilities

Roger Webb, Executive Director
Martha Cantu, Operations Director
Patrice LeBlanc, Grants Management Director

Oversight Agencies

Michael Sparks
Governor's Office of Budget, Planning, and Policy
internalaudits@governor.state.tx.us

Ed Osner
Legislative Budget Board
Ed.Osner@lbb.state.tx.us

Internal Audit Coordinator
State Auditor's Office
iacoordinator@sao.state.tx.us

Ken Levine
Sunset Advisory Commission
sunset@sunset.state.tx.us



TEXAS COUNCIL FOR DEVELOPMENTAL DISABILITIES

INTERNAL AUDIT REPORT #2010-1

Information Security Standards – TAC 202

Presented to
TCDD Audit Committee
October 18, 2010

Prepared by:
Rupert & Associates, PC
Certified Public Accountants
Austin, Texas

Table of Contents

Internal Auditor’s Report..... 1

Executive Summary 2

Audit Results and Recommendations 3

 Internal Audit Objectives -

 Compliance 5

 Procedures..... 6

 Oversight & Monitoring 7

 Audit Recommendations..... 8

Follow Up on Prior Audit Recommendations10

Report Distribution Page..... 11

Acronyms and Abbreviations

- BCP Business Continuity Plan
- BCPG Business Continuity Planning Guidelines (DIR publication)
- BIA Business Impact Analysis
- CPA Comptroller of Public Accounts, Texas
- DIR Department of Information Resources, Texas
- DRP Disaster Recovery Plan
- DSA Designated State Agency
- IIA Institute of Internal Auditors, International
- ISAS Integrated Statewide Administrative System
- ISO Information Security Officer
- ITS Information Technology Security
- OP Operating Procedure
- SAO State Auditor’s Office, Texas
- TAC Texas Administrative Code
- TCDD Texas Council for Developmental Disabilities
- TEA Texas Education Agency
- TGC Texas Government Code



Internal Audit Report

August 6, 2010

Audit Committee and Board Members
The Texas Council for Developmental Disabilities

The following report provides the results and recommendations noted during the internal audit procedures conducted in fiscal year 2010. Included in this report are the purpose, scope, results, and recommendations of the audit, as well as management's responses to those recommendations.

The internal audit was conducted in accordance with the Institute of Internal Auditor's (IIA) *International Standards for the Professional Practice of Internal Auditing*, the Government Accountability Office's (GAO) *Government Auditing Standards*, and the Texas Internal Auditing Act. We believe that our work fully supports our conclusions.

This report is distributed to and intended for the use of the Texas Council for Developmental Disabilities management and Governing Board, and the oversight agencies as identified in the Texas Internal Audit Act.

Rupert & Associates, P.C.

Certified Public Accountants
Austin, Texas

Executive Summary

Audit Purpose

The Texas Council for Developmental Disabilities' (TCDD) annual internal audit plan is risk-based, with specific audit areas and objectives determined after an annual risk assessment update is conducted by management and the internal auditor. The Internal Audit plan developed for TCDD for fiscal year 2010 consisted of the following objectives:

1. Information Technology: Assess TCDD's compliance with Title 1, Part 10, Chapter 20, Texas Administrative Code (TAC 202), Information Security Standards. This audit will also satisfy the requirement for a periodic audit of TCDD's major systems and controls, including safeguarding of assets and data. Additional audit activity may include to consult, advise, and monitor the development and refinement of the grantee reporting database, as needed.
2. Follow up on prior audit recommendations.

Key Observations

1. The Texas Education Agency (TEA), as the designated state agency for TCDD, is responsible for overall compliance with TAC 202. TEA has not had a TAC 202 audit specifically, but they have had multiple other audits that included various information security objectives. These previous audits have not identified any significant problems with TEA's information technology (IT) security. TEA provided written operating procedures that address DIR's requirements for IT security policies. These policies include specific steps that are the responsibility of TEA divisions.
2. TCDD has policies and procedures in place to ensure that they comply with TEA's operating procedures as they relate to information security. Some of the procedures were revised during the audit to adhere to agency division responsibilities according to TEA procedures.
3. TEA's oversight activities over TCDD's information security standards should be clarified. TCDD should coordinate with TEA to identify responsibilities of TEA and of TCDD to ensure that TCDD has adequate processes for the protection of their independent assets and activities.
4. All prior audit recommendations have been addressed by TCDD.

Significant Recommendations

- | | |
|--------|---|
| 2010-1 | Develop a Business Recovery Plan tailored to TCDD |
| 2010-2 | Promote internet security training among TCDD staff |
| 2010-3 | Work with TEA to ensure oversight of TCDD's IT security processes |

Audit Results and Recommendations

BACKGROUND & PURPOSE

Texas Administrative Code Chapter 202 (TAC 202), Subchapter B, defines information security standards for state agencies. The Code covers things such as security standards policies, management and staff responsibilities, managing security risks, business continuity planning, user security practices, and more.

The Memorandum of Understanding between TEA and TCDD calls for TEA to provide information technology support services that “includes desktop and laptop computers, printers, networking, server and infrastructure. E-mail accounts, network connection (including LAN equipment and data circuits), and related hardware and software. TEA support shall be provided in a manner that assures separate identity for TCDD computer functions including website (www.txdcc.state.tx.us) and email (e.g. Roger.Webb@tcdd.state.tx.us).”

TCDD relies on their designated state agency, TEA, to provide guidance and consultation necessary to comply with state requirements include TAC 202. TCDD in turn is responsible to coordinate with TEA as requested to ensure successful compliance with the Code. The purpose of this audit was to identify compliance requirements and determine where responsibilities fall between TCDD and TEA in order to evaluate if processes in place at TCDD are sufficient to ensure that responsibilities for security standards are met.

“Business continuity planning provides a quick and smooth restoration of operations after a disruptive event. Business continuity planning is a major component of risk management. Business continuity planning includes business impact analysis, business continuity plan (BCP) development, testing, awareness, training, and maintenance.

Traditionally, disaster recovery planning has focused on computer systems. Because mission-critical functions inevitably depend on technology and telecommunications networks, rapid recovery of these is of little value without also recovering business unit operations. Mainframe and minicomputer systems usually have reliable recovery plans.

Today, however, many critical applications have migrated to distributed, decentralized environments with less rigid controls. Recovering functional processes includes more than just information systems—consideration needs to be given to such items as 800 and long distance service, locations for employees to work, the salvage of building contents, and so forth.

As with an insurance policy, it is hoped that a business continuity plan is never needed for a real disaster. Keep in mind that a BCP not maintained can be worse than no plan at all. An agency’s ability to recover mission-critical processes, resume operations, and eventually return to a normal business environment can be considered a major asset. Thorough planning can reduce liability, disruption to normal operations, decision making during a disaster, and financial loss. And equally important to state government, it can provide continued goodwill and service to the state’s citizens.”¹

¹ Department of Information Resources – Business Continuity Planning Guide

CRITERIA

TAC 202 – Information Security Standards
DIR’s Business Continuity Planning Guide and Business Impact Analysis
TEA Operating Procedure 09-01 Business Continuity Planning
TEA Operating Procedures 10-01 through 10-13 (various IT Security OPs)
TCDD Operating Procedure 01-11 Business Continuity Plan
TCDD Operating Procedure 01-15 Adopt Various TEA OPs
Memorandum of Understanding - TCDD and TEA

SCOPE, METHODOLOGY, & OBJECTIVES

The scope of the audit included an evaluation of the information security processes to ensure safeguarding of assets and information in compliance with TAC 202 at TCDD and their designated state agency, TEA. The scope was limited to considering processes in place during fiscal year 2010.

The audit methodology included interviews, questionnaires, and discussions with various personnel at TEA and TCDD. Background information was obtained from review of the TAC 202 and the Department of Information Resources website. This information provided the basis for compliance criteria. Information was obtained from TEA through questionnaires and communications with the Information Security Officer, the ITS Planning and Special Projects Manager, the Director of Agency Infrastructure, and the Director of Internal Audit.

TEA Operating Procedures (OP) that relate to information security and TAC 202 were reviewed and responsibilities specific to TCDD were identified for testing compliance. TCDD’s operating procedures as they relate to information security were also reviewed and the Operations Director provided responses to questionnaires and audit inquiries.

The general audit objective was to assess information security controls and procedures in place to determine:

- A. What are the roles and responsibilities of TCDD and TEA as it relates to TAC 202 compliance?
- B. Does TCDD have adequate procedures in place to ensure that they meet their responsibilities as defined by TEA’s information security procedures?
- C. Does TEA provide adequate monitoring and oversight of TCDD information security control processes to meet the IT security standards?

AUDIT RESULTS BY OBJECTIVE

Audit Objective A: What are the roles and responsibilities of TCDD and TEA as it relates to TAC 202 compliance?

Results and Conclusions:

TAC 202 Subchapter B is the State of Texas' Security Standards Policy that applies to all state agencies.

TEA as the designated state agency (DSA) for TCDD is responsible for agency-level compliance with TAC 202. TEA has written procedures and other guidance to ensure TAC 202 compliance. Within these procedures is guidance to agency divisions and division directors on specific steps they need to take to ensure their information assets are adequately protected and agency-wide compliance with information security standards is accomplished. For IT security purposes, TEA considers TCDD to be a division of the agency, and is thus responsible for assisting TCDD to address the expected division-level activities as appropriate to ensure that the agency as a whole meets the information security objectives of the TAC 202.

In accordance with the interagency MOU, TEA provides IT support services that include desktop and laptop computers, printers, networking, server and infrastructures, e-mail accounts, network connection, and related hardware and software in addition to data security and recovery services. Even though TCDD is not truly a 'Division' of TEA, in order to support the overall objectives of TEA security measures, they should have their own security procedures that interface with and support the overall agency effort.

TEA OP 09-01 'Business Continuity Planning' establishes procedures for agency-wide business continuity planning 'in order to ensure the quick and effective recovery of mission-essential business functions in the event of a disaster or major business interruption'. This procedure applies to all agency divisions and employees. Each division is to develop, test, maintain, and be prepared to implement comprehensive business recovery plans for the purpose of restoring all mission-critical business functions to operational status as quickly and effectively as possible.

TEA OP 10-01 'Acquisition and Disposal of Information Technology Resources' requires division director's to plan, budget and purchase computer peripheral equipment requirements in advance and report on the Semi-Annual IT Procurement Planning Report. This procedure was adopted by TCDD in a prior year in their OP 01-15.

TEA OP 10-02 'Computer Room Security' addresses access controls to the TEA onsite computer room. This OP was recently adopted by TCDD in their revision of OP 01-15 to address physical access to their computers.

Texas Council for Developmental Disabilities (TCDD)
Internal Audit Report FY-2010

TEA OP 10-10 'Information Systems Intrusion Detection Policy' provides direction on ways to protect against intrusion incidents. This policy calls for users to be trained to report anomalies in systems performance and signs of suspected intrusions to the ISO. Staff at TCDD have attended TEA training, including classes to recognize system incidents for reporting. This procedure was also recently adopted by TCDD in the revision of their OP 01-15.

Other TEA operating procedures in place to define agency controls to ensure the safety of information assets include:

TEA OP-10-03	Confidential Enterprise Information
TEA OP-10-04	Information Resources Access and Acceptable Use
TEA OP-10-08	Information Resources Security Controls
TEA OP-10-09	Mail and Instant Messaging Policy
TEA OP-10-11	Information Security Incident Response Policy

In addition to the operating procedures, TEA has a written business continuity plan (BCP) that provides more guidance on how divisions might address the information security standards. The TEA BCP goes into more depth and offers up for consideration items such as emergency fire boxes with supplies; emergency contact lists; a list of critical resources that should be retrieved if the facility becomes accessible; alternate facility operations facilities (logistics; space and equipment); etc. The TEA BCP, Section 2.2.9 on Business Recovery, suggests the following activities -

- Essential functions - what would be the first 3 to 5 things people would do in their department following a business disruption?
- Business Impact Analysis – identify all functions and assess their criticality. Types of criteria include customer service; internal operations; legal / statutory, and financial – prioritize from mission-critical to non-critical.
- TEA Division Directors are directly responsible for the continuity and recovery of the business functions their divisions perform and are expected to establish business continuity planning processes commensurate with their importance to the agency.
- Division Directors will develop a division business resumption plan that includes written procedures, documentation, and other information sufficient to ensure full recovery of the division's mission-essential files, records, and business function in the event of a disaster.

Audit Objective B: Does TCDD have adequate procedures in place to ensure that they meet their responsibilities as described in TEA's information security procedures?

Results and Conclusions:

TCDD has an OP 01-11 Business Continuity Planning to ensure the quick and effective recovery of mission-essential business functions in the event of a major business interruption. The procedure defines its purpose, scope, and objective, and identifies

Texas Council for Developmental Disabilities (TCDD)
Internal Audit Report FY-2010

authoritative parties and their respective responsibilities. In April of this year, this operating procedure was reviewed by staff and directors' responsibilities were more clearly stated.

TCDD adopts various TEA procedures in OP 01-15, as discussed in the previous section. There are various other operating procedures adopted under this OP that do not relate to IT security; the IT related OPs that have been adopted include:

TEA OP-10-01	Acquisition and Disposal of Information Technology Resources
TEA OP-10-03	Confidential Enterprise Information
TEA OP-10-04	Information Resources Access and Acceptable Use
TEA OP-10-08	Information Resources Security Controls
TEA OP-10-09	Mail and Instant Messaging Policy
TEA OP-10-11	Information Security Incident Response Policy

In April of this year TCDD reviewed this operating procedure and adopted these additional TEA procedures.

TEA OP-10-02	Computer Room Security
TEA OP-10-10	Information Systems Intrusion Detection Policy

For purposes of IT security, TCDD, as a 'division' of TEA should be performing certain additional security activities described in TEA procedures. TCDD should consider adopting additional TEA procedures or strengthening existing procedures. The TEA OP 09-01 Business Continuity Planning, Section 5(f) discusses various division level responsibilities for continuity and recovery of the division's business functions. These elements should be reviewed and incorporated as appropriate to TCDD circumstances.

Disaster recover planning has traditionally focused on computer systems, but business recovery requires responsibilities significantly different from those of the information security function. The DIR Business Continuity Planning Guide provides guidelines for a business recovery plan that outlines the roles and responsibilities associated with these planning activities.

Audit Objective C: Does TEA provide adequate monitoring and oversight of TCDD information security control processes to meet the IT security standards?

Results and Conclusions:

Monitoring and oversight at TEA includes data security procedures provided to the divisions of the agency. The BCP defines certain monitoring steps over divisions – such as section 2.2.9.1 which calls for the Division of Agency Infrastructure to be responsible for maintenance and disposition of agency public records - all records and/or files in whatever medium created or stored by the agency. This includes:

Texas Council for Developmental Disabilities (TCDD)
Internal Audit Report FY-2010

- identifying mission critical business functions and processes;
- identifying the individual with primary responsibility;
- a statement of systems dependency;
- a customer service impact rating;
- operation impact of the process; and
- developing a functional recovery plan for continuation of processes in the absence of automated systems.

TEA is also responsible for incident reporting, intrusion testing, and software audits. TEA has included TCDD incident reporting in their monthly statistics report to DIR, but they have not performed any software audits or intrusion testing. To be proactive, TCDD staff should be aware of how to recognize possible intrusions or incidents for reporting to TEA. Software audits at TCDD could be delegated internally with a report provided to TEA. This is an example of the type of activity that TCDD could delegate internally and provide a report to TEA. TEA offers a series of eight internet security classes. TCDD should encourage staff to attend as many classes as possible to raise the staff level of awareness on these security issues.

TEA's MOU provides for certain IT services to TCDD, but the extent of responsibility for IT security support is not mandated and should be addressed to ensure adequate IT security at TCDD. The interagency MOU should be revisited to clearly define the responsibilities for these procedures.

AUDIT RECOMMENDATIONS & MANAGEMENT RESPONSES

Recommendation 2010-1:

Develop a written Business Recovery Plan for TCDD that will interface with TEA efforts for systems and business recovery in the event of an incident. There are resources available through TEA and DIR to guide users on various elements to be considered in the development of a plan. The objective of the document is to ensure that necessary procedures to address the business recovery needs of the entity in the event of an incident have been identified, are thoroughly thought out, are comprehensive, and are appropriately documented and communicated to staff.

Management Response 2010-1:

TCDD has adopted Operating Procedure 01-11 Business Continuity Planning that establishes procedures for TCDD business continuity planning in order to ensure the quick and effective recovery of mission-essential business functions in the event of a disaster or major business interruption that impairs the operations of the TCDD.

In addition, TCDD IT functions are included in the TEA Business Continuity Plan version 1.0 dated January 2010. TCDD will review this matter further with TEA to

determine if additional information is needed by TEA to restore TCDD IT functions should that be necessary.

TCDD has recently developed and adopted an Emergency Backup Succession Plan to address organizational stability and leadership continuity of the Executive Director and key management staff.

Recommendation 2010-2:

Agency policy calls for employees to sign an acknowledgement of appropriate usage policy at the time of hire. In addition to this initial acknowledgement, TCDD should encourage a reiteration of the risks of inappropriate technology usage. TEA could be asked to provide their internet security class to all TCDD staff in a series of classes. The series would serve to raise awareness and reinforce appropriate usage policies.

Management Response 2010-2:

TEA currently offers security classes through their Office of Organizational Effectiveness. These classes are open to TCDD staff. TCDD staff receive emails regarding security class curriculum and schedules. TCDD staff is encouraged to sign up for these classes to raise security awareness and reinforce security usage. Several TCDD staff have taken advantage of security classes offered by TEA and have shared information with other TCDD staff. Appropriate use of technology is discussed periodically during TCDD staff meetings.

Recommendation 2010-3:

TCDD should work with the TEA ISO to identify the level of security support to be provided by TEA and the activities for which TCDD is responsible. The interagency MOU should be revisited to clearly define the responsibilities for these procedures, including IT security oversight.

Management Response 2010-3:

By TEA IT protocols, TCDD staff do not have “administrative rights” for TCDD computers. TEA is responsible for all software installation on TCDD computers and related software audits and intrusion testing and reporting. TCDD believes the responsibilities of TEA and of TCDD related to IT services and security are clear and appropriate within the current MOU. The MOU defines the information technology support provided for TCDD by TEA, including support through the Department of Information Resources and the state Data Center Service. It includes support to desktop and laptop computers, printers, networking, server and infrastructure, E-mail accounts, network connection (including LAN equipment and data circuits) and related hardware and software. In addition, TCDD works with the ISO to determine costs and services associated with DIR/DCS Server Infrastructure, E-mail accounts, and services provided by Northrop Grumman for desktops and laptops.

Follow Up on Prior Audit Recommendations

2009-1 Contract Management Audit

Recommendation 2009-1-1-1: TCDD procedures for contracts should be reviewed and updated on a regular basis. Procedures should include monitoring controls to ensure performance of procedures as written. A checklist for contractor files would help ensure completeness of files and compliance with procedures.

COMPLETED – Operating procedures were updated in August of 2009 to reflect changes recommended related to review and update of procedures and contract management responsibilities.

Recommendation 2009-1-2-1: The State's TPASS Contract Management Guide recommends keeping one complete master Contract Administration File for the life of each contract. The file will provide a basis for settling claims and disputes should they arise in administrative or court actions.

COMPLETED – One contract file per contract is being maintained by the Operations Director. Contract files will be kept in accordance with the TCDD records retention schedule. A file checklist, a performance evaluation, and a monitoring document tool were all developed per the suggested Appendix 11.

Recommendation 2009-1-2-2: For bid solicitations, the documentation supporting the vendor selection process should be consistent with the TEA Contract Manual's recommended documentation.

COMPLETED – Bid proposal documentation and supporting material will be kept in the contract file, if there is any.

Recommendation 2009-1-3-1: The compilation of vendor performance documentation maintained in the contract administration files, as discussed in a previous recommendation, would enable TPASS Vendor Performance Forms reporting for contracts that meet the threshold or performance criteria for reporting in the VPTS.

COMPLETED – TCDD will use the contract evaluation tool and will consult with TEA to determine when it is appropriate to report to the VPTS.

Recommendation 2009-1-4-1: TCDD procedures should be reviewed and updated on a regular basis, including a process for monitoring controls, direction to follow the TEA Contract Manual, and guidance regarding documentation and approvals.

COMPLETED – OP 01-08 has been updated to implement this recommendation.

REPORT DISTRIBUTION PAGE

Texas Council for Developmental Disabilities, Audit Committee

Mary Durham, Chair
John Morris, Vice-Chair
Andrew Crim, Member
Marcia Dwyer, Member
Brenda Coleman-Beattie, Council Chair

Texas Council for Developmental Disabilities

Roger Webb, Executive Director
Martha Cantu, Operations Director
Patrice LeBlanc, Grants Management Director

Oversight Agencies

Michael Sparks
Governor's Office of Budget, Planning, and Policy
internalaudits@governor.state.tx.us

Ed Osner
Legislative Budget Board
Ed.Osner@lbb.state.tx.us

Internal Audit Coordinator
State Auditor's Office
iacoordinator@sao.state.tx.us

Ken Levine
Sunset Advisory Commission
sunset@sunset.state.tx.us



TEXAS COUNCIL FOR DEVELOPMENTAL DISABILITIES

INTERNAL AUDIT PLAN

Fiscal Year 2011

Prepared by:
Rupert & Associates, PC
Certified Public Accountants
Austin, Texas

Table of Contents

Letter to Council Members	1
Section 1: Risk Assessment.....	2
Section 2: Internal Audit Plan	4
Section 3: History of Internal Audits at TCDD.....	5
Exhibit 1: Risk Footprint	6
Distribution Page	7



RUPERT & ASSOCIATES
CERTIFIED PUBLIC ACCOUNTANTS

September 21, 2010

Members of the Council,
Texas Council for Developmental Disabilities (TCDD)

The following document presents the proposed fiscal year 2011 Internal Audit Plan for your review and approval, in accordance with the Texas Internal Auditing Act.

Chapter 2102 of the Government Code requires that the internal audit plan be risk-based and include areas identified through a risk assessment process. This document presents the risk assessment results, the proposed audit plan, and a summary of the internal audits performed in prior years at TCDD.

The FY 2011 Internal Audit Plan that follows is submitted for your approval.

Respectfully,

Rupert & Associates, PC

Certified Public Accountants
Austin, Texas

Section 1: RISK ASSESSMENT

This section presents the update of the Texas Council for Developmental Disabilities (TCDD) Risk Assessment for FY 2011, and establishes the foundation for the Internal Audit Plan presented in the next section.

TCDD continues to refine Grants Administration procedures for monitoring grantee performance, and TCDD staff also continues to participate in the design and development of the DD Suite – an electronic grantee reporting database – in conjunction with DD Councils from other states.

The risk assessment update process was performed by TCDD management and facilitated by the internal auditor in September of 2010. Management continues to exhibit a commitment to improving operational efficiencies and performance, including their voluntary participation in and responsiveness to the internal audit function.

Purpose

The TCDD risk assessment provides management and board members with a prioritized list of risks associated with their activities. From these risks, a management strategy is developed. The risk assessment allows the Board to identify the risks being monitored by management and evaluate the effectiveness of controls and responses to those risks.

Concepts of Risk

Risk is defined as the level of exposure to uncertainties that an agency must comprehend and manage to effectively and efficiently achieve its objectives and execute its strategies. Risk is a measurement of the likelihood that an organization's goals and objectives will not be achieved. Controls are anything that improves the likelihood that goals and objectives will be achieved.

Methodology

The Texas Council for Developmental Disabilities' risk assessment process includes three parts: (1) identifying agency activities; (2) identifying and rating risks for each activity; and (3) identifying actions to mitigate risks. The risk assessment update contemplates additional risks to be added and also considers additional controls put in place. The risk assessment update is used to determine the highest risk areas for the current year's audit plan.

Risk Footprint

The attached risk assessment footprint reflects the prioritized risks as identified and ranked in the current year's risk assessment update. Each risk identified in the matrix is assigned two risk factors of High, Medium, or Low based on the impact the risk would have on the agency if it occurred and the probability of occurrence. By combining these measures the agency develops a priority ranking for each risk factor. The following key provides the level of risk management that will be employed by the agency for each potential risk factor ranking:

- HH, HM – Extensive Risk Management that includes monitoring by management and an internal audit.
- HL, MH – Considerable Risk Management that includes monitoring by management and a less in depth audit.
- MM, ML, LH – Manage and monitor the risk
- LM, LL – Monitor or accept the risk

Results

The results of the risk assessment shown in Exhibit 1 illustrate changes in the prioritization and organization of consolidated activities and risk factor priorities based on the current year's update. The highest-risk areas are marked in red and, as in the prior year, relate to activities in Grant Administration, Executive and Administrative functions, and the Public Policy and Information area.

Risks in the red area require oversight controls to ensure that the supervisory and operating controls are working. Oversight controls can include exception reports, status reports, analytical reviews, variance analysis, etc. These controls are performed by representatives of executive management, on information provided by supervisory management. Areas within this highest risk category should also be considered for inclusion in the internal audit plan.

Activities that fall within the yellow risk category require considerable risk management. Under this category of risk executive management or their designees should perform oversight controls to ensure that supervisory and monitoring controls are working. If internal audit provides services in this area, it is to ensure that oversight of the supervisory controls are appropriate and are being performed.

The last two categories of risk are marked in green and gray. Risks falling within the green areas rely on department managers to provide oversight by ensuring that supervisory controls and operating controls are working. Department managers should report to the Executive Director on the condition of these risks. Risks in the gray area are low risk areas that are managed by operating and supervisory controls and executive management accepts the residual risk in these areas.

Section 2: FY 2011 INTERNAL AUDIT PLAN

The Texas Internal Auditing Act requires certain audits to be performed on a periodic basis. Required audits include audits of the department's accounting systems and controls, administrative systems and controls, electronic data processing systems and controls, and other major systems and controls.

The *International Standards for the Professional Practice of Internal Auditing* requires the internal audit activity to evaluate the effectiveness and contribute to the improvement of risk management processes. The internal audit activity must evaluate risk exposures, including the potential for the occurrence of fraud and how it is managed. The auditor assists the organization in maintaining effective controls by evaluating the effectiveness and efficiency of the risk management process and by promoting continuous improvement. Specifically, the internal audit activity must evaluate the adequacy and effectiveness of controls in responding to risks within the organization's governance, operations, and information systems regarding the:

- Reliability and integrity of financial and operational information,
- Effectiveness and efficiency of operations,
- Safeguarding of assets, and
- Compliance with laws, regulations, and contracts.

Internal auditors are required to ascertain the extent to which management has established adequate criteria to determine whether objectives and goals have been accomplished.

Based on the updated risk assessment, the proposed internal audit focus for FY-2011 is:

1. Grantee Monitoring: Review and evaluate current grantee monitoring procedures and controls. As needed, consult, advise, and monitor the development and refinement of the grantee reporting database (DD Suite).
2. Follow up on prior year audit recommendations.

Alternative audit areas are proposed in the event that circumstances prevent the implementation of the planned audit, or if additional resources are available for more audit work. An alternative audit area proposed is IT security over social media sites.

**Section 3:
HISTORY OF
INTERNAL AUDITS AT TCDD**

2010	Information Security TAC 202
2009	Contract Administration and Management Quality Assurance Review
2008	Grantee Audit Desk Review Process Internal Controls over Financial Reporting to Council Grantee Records Management Process (database and hard copy files)
2007	Grantee Monitoring: Onsite Review Process Internal Administrative Operating Procedures Grantee Reporting Database Development (DD Suite)
2006	Control Environment Evaluation Grantee Expenditure Monitoring Public Policy Processes and Controls Administrative Policies and Procedures
2005	Grantee Risk Assessment Model Evaluation Master Grantee Records Maintenance Process Fraud Prevention and Reduction Policy Administrative & Project Development Procedures
2004	Follow-up on MATRS Review Findings Grantee Risk Assessment Model Development Electronic Grants Manual Review
2003	Grants Manual Compliance Review TRC Performance Audit Review
2002	Grants Administration

Report Distribution Page

Texas Council for Developmental Disabilities, Audit Committee

Mary Durham, Chair
John Morris, Vice-Chair
Andrew Crim, Member
Marcia Dwyer, Member
Brenda Coleman-Beattie, Council Chair

Texas Council for Developmental Disabilities

Roger Webb, Executive Director
Martha Cantu, Operations Director
Patrice LeBlanc, Grants Management Director

Oversight Agencies

Michael Sparks
Governor's Office of Budget, Planning, and Policy
internalaudits@governor.state.tx.us

Ed Osner
Legislative Budget Board
Ed.Osner@lbb.state.tx.us

Internal Audit Coordinator
State Auditor's Office
iacoordinator@sao.state.tx.us

Ken Levine
Sunset Advisory Commission
sunset@sunset.state.tx.us