AUDIT AND FINANCE COMMITTEE MEETING BOOK OF SEPTEMBER 7, 2017

Sharon Thomason, Chair
Paul Braden, Member
Asusena Reséndiz, Member
Leo Vasquez, III, Member

AGENDA
8:00 AM
SEPTEMBER 7, 2017

JOHN H. REGAN BUILDING
JHR 140, 105 W 15TH STREET
AUSTIN, TEXAS 78701

CALL TO ORDER, ROLL CALL   **Sharon Thomason, Chair**

CERTIFICATION OF QUORUM   **Sharon Thomason, Chair**

The Audit and Finance Committee of the Governing Board of the Texas Department of Housing and Community Affairs will meet to consider and may act on any of the following:

ACTION ITEMS:

ITEM 1: Presentation, discussion, and possible action to Approve Audit Committee Minutes Summary for June 29, 2017
Mark Scott
Director of Internal Audit

ITEM 2: Presentation, discussion, and possible action to Approve the Fiscal Year 2018 Internal Audit Work Plan
Mark Scott
Director of Internal Audit

REPORT ITEMS:
Mark Scott
Director of Internal Audit

1. Presentation and discussion of the Internal Audit: Review of the Information Systems Division

2. Status of 2017 Audit Plan

3. Discussion of Recent External Audit Activity

4. Status of Peer Review

PUBLIC COMMENT ON MATTERS OTHER THAN ITEMS FOR WHICH THERE WERE POSTED AGENDA ITEMS.

EXECUTIVE SESSION
The Committee may go into Executive Session (close its meeting to the public) on any agenda item if appropriate and authorized by the Open Meetings Act, Tex. Gov't Code, Chapter 551 and under Tex. Gov't Code, §2306.039.

1. Pursuant to Tex. Gov't Code, §551.074 the Audit Committee may go into Executive Session for the purposes of discussing personnel matters including to deliberate the appointment, employment, evaluation, reassignment, duties, discipline, or dismissal of a public officer or employee.

2. Pursuant to Tex. Gov't Code, §551.071(1) the Committee may go into executive session to seek the advice of its attorney about pending or contemplated litigation or a settlement offer.

3. Pursuant to Tex. Gov't Code, §551.071(2) the Committee may go into executive session for the purpose of seeking the advice of its attorney about a matter in which the duty of the attorney to the governmental body under the Texas Disciplinary Rules of Professional Conduct of the State Bar of Texas clearly conflicts with Tex. Gov't Code, Chapter 551.

4. Pursuant to Tex. Gov't Code, §2306.039(c) the Committee may go into executive session to receive reports from the Department's internal auditor, fraud prevention coordinator, or ethics advisor regarding issues related to fraud, waste or abuse.

OPEN SESSION

If there is an Executive Session, the Committee will reconvene in Open Session and may take action on any items taken up in Executive Session. Except as specifically authorized by applicable law, the Audit Committee may not take any actions in Executive Session.

ADJOURN

To access this agenda and details on each agenda item in the board book, please visit our website at *www.tdhca.state.tx.us* or contact Mark Scott, TDHCA Internal Audit Director, 221 East 11th Street Austin, Texas 78701-2410, 512.475-3813 and request the information.

Individuals who require the auxiliary aids, services or sign language interpreters for this meeting should contact Gina Esteves, ADA Responsible Employee, at 512-475-3943 or Relay Texas at 1-800-735-2989 at least two (2) days before the meeting so that appropriate arrangements can be made.

Non-English speaking individuals who require interpreters for this meeting should contact Annette Cornier 512-475-3803 at least three (3) days before the meeting so that appropriate arrangements can be made.

Personas que hablan español y requieren un intérprete, favor de llamar a Annette Cornier al siguiente número 512-475-3803 por lo menos tres días antes de la junta para hacer los preparativos apropiados

NOTICE AS TO HANDGUN PROHIBITION DURING THE OPEN MEETING OF A GOVERNMENTAL ENTITY IN THIS ROOM ON THIS DATE:

Pursuant to Section 30.06, Penal Code (trespass by license holder with a concealed handgun), a person licensed under Subchapter H, Chapter 411, Government Code (handgun licensing law), may not enter this property with a concealed handgun.

De acuerdo con la sección 30.06 del código penal (ingreso sin autorización de un titular de una licencia con una pistola oculta), una persona con licencia según el subcapítulo h, capítulo 411, código del gobierno (ley sobre licencias para portar pistolas), no puede ingresar a esta propiedad con una pistola oculta.

Pursuant to Section 30.07, Penal Code (trespass by license holder with an openly carried handgun), a person licensed under Subchapter H, Chapter 411, Government Code (handgun licensing law), may not enter this property with a handgun that is carried openly.

De acuerdo con la sección 30.07 del código penal (ingreso sin autorización de un titular de una licencia con una pistola a la vista), una persona con licencia según el subcapítulo h, capítulo 411, código del gobierno (ley sobre licencias para portar pistolas), no puede ingresar a esta propiedad con una pistola a la vista.

NONE OF THESE RESTRICTIONS EXTEND BEYOND THIS ROOM ON THIS DATE AND DURING THE MEETING OF THE AUDIT COMMITTEE OF THE TEXAS DEPARTMENT OF HOUSING AND COMMUNITY AFFAIRS.

ACTION ITEMS

Presentation, discussion and possible action on Audit and Finance Committee Meeting Minutes Summary for June 29, 2017.

RECOMMENDED ACTION

RESOLVED, that the Audit and Finance Committee Meeting Minutes Summary for June 29, 2017 are hereby approved as presented.

MINUTES OF THE AUDIT and FINANCE COMMITTEE
OF THE GOVERNING BOARD OF THE
TEXAS DEPARTMENT OF HOUSING AND COMMUNITY AFFAIRS

On Thursday, June 29th, 2017, at 8:00 a.m. the meeting of the Audit and Finance Committee (the "Committee") of the Governing Board (the "Board") of the Texas Department of Housing and Community Affairs ("TDHCA" or the "Department") was held in the John H. Reagan Building, Room JHR 140, at 105 W 15th street, Austin, Texas. Sharon Thomason presided over the meeting, and Mark Scott served as secretary. Committee members Sharon Thomason, Paul A. Braden, Asusena Resendiz, and Leo Vasquez were in attendance and represented a quorum for the committee meeting.

The minutes of the January 26th, 2017 meeting of the Committee were adopted and presented for approval.

Mrs. Thomason started the meeting by introducing new Board and Committee members; Mr. Vasquez, Ms. Resendiz, and Mr. Braden.

After approval of the meeting minutes of January 26th, 2017 Mr. Scot presented the internal audit report of the Low Income Housing Tax Credit program. This was a base and first comprehensive audit of the program and covered activities in the TDHCA Multifamily Division and Asset Management Division. Some areas for improvements were identified and were discussed with Program management. The audit included description of the costs of the program and the returns to the investors, policies and procedures, and also visits to several of the tax credit properties. It also included cost certification process and issuance of IRS forms. The attributes that were tested were in compliance with established procedures.

Mr. Scott then gave an update on internal audit's activities. He stated that OIA is currently performing a comprehensive audit of IT which will also be a base audit. The other two audits remaining on the FY2017 audit plan are Bond Finance and the Contract For Deed Conversion (CFDC) Programs. The next item was an update on the procurement for a Peer Review. Request For qualification (RFQ) has been posted on the agency's website and also on the Texas Register.

Other activities that internal audit was involved in included various consulting activities and participation in agency workgroups in an ex officio manner. The consulting activities are in regard to sub-recipients who are also subject to Single Audit Act. This is in addition to being on the Fraud, Waste and Abuse Committee within the agency.

External audit activities include the ongoing statewide annual audit of the agency's financial statements. On the federal compliance part of the statewide audit KPMG did not select TDHCA programs as "major programs" to audit this year, however they'll follow up on the LIHEAP program audit that had a finding in 2016. HUD auditors conducted an audit of the agency for compliance with Davis-Bacon requirements earlier this year and will be issuing their report soon.

Mrs. Thomason concluded the audit portion of the meeting and moved to the next item on the agenda; Financial Administration Division. Mr. David Cervantes, the TDHCA's CFO began his presentation.

Mr. Cervantes started his presentation by introducing his key staff involved in the budget process and coordination throughout the department. Ernie Palacios is the director of Financial administration, Kristina Vavra is the manager for budget for travels and payroll operations, and the most recent member is Paul Ford. He's senior financial analyst and joined the department less than a year ago. Mr. Cervantes then gave a brief description and background on the biennial budget process throughout the state government.

Mr. Cervantes continued by saying that the budget presented deals with operations of the Department and aligns with the General Appropriations Act.

Mr. Vasquez asked if there is anything on the call for the special session that would specifically impact this budget? Mr. Cervantes responded that we're not aware of anything particular to Senate Bill 1, and the bill is signed by the governor.

Mr. Palacios said that over the last four months they've been meeting with division directors and managers to develop an internal operating budget for FY2018. The internal operating budget provided includes a comparison report with the 2017 operating budget. He then gave an explanation of the budget, changes from the previous fiscal year, and the contributing factors to the changes.

Mr. Palacios then provided an explanation of the Housing Finance Division budget. This subset of the budget is specific to the fees that are generated through different programs.

Mr. Vasquez asked about the comparison between last year and this year's budget, and the primary driver for the change. Mr. Palacio responded that the budget has increased by $828,000 and it's due to the capital budget and the FTEs.

Mrs. Thomason asked for votes to recommend approval to the full board. With no objections both budgets were recommended to the full board for approval.

Mr. Irvine said that we've a very complex array of funding sources which carry specific restrictions and rules. The Finance Division is responsible for ensuring that these funds are in compliance with all applicable rules and regulations. Krissy oversees a very complex timekeeping system that manages the recordkeeping used by federal agencies when auditing a specific program. Mr. Irvine also explained the difference between the budget and funding in business world versus state and federal, and how these funds are collected, kept, and moved into and out of the state treasury for use by the agency. He stated that little over one percent that is in the budget for salary and equity adjustments, reclassifications and merit adjustments, is actually very small relative to the challenge they face, and that he hoped at a future meeting we can get into some of the agency's philosophy about compensation and draw on Committee member's ideas for ways to improve the compensation structure.

As far as Internal Audit and consulting engagements goes Mr. Irvine stated that the consulting work Mark and his team provide are just phenomenally valuable. The agency is audited constantly and scrutinized by hundreds of very knowledgeable people, in addition to the audits by the State Auditor's Office and KPMG and so forth. He emphasized the importance of internal audit and its unique position in being independent and reporting to the Committee but yet working with the agency staff on a daily bases and understanding their work.

Mrs. Thomason thanked Mr. Irvine and asked if there were any questions from the Audit Committee members. With no questions the meeting was adjourned at 8:23am

2

Presentation, discussion, and possible approval of the Fiscal Year 2018 Internal Audit Work Plan

RECOMMENDED ACTION

WHEREAS, the Tex. Gov't Code §2306.073(b), the Internal Auditing Act and audit standards require the Department's Governing Board to approve an annual audit work plan that outlines the internal audit projects planned for the fiscal year;

WHEREAS, Staff has presented a Fiscal Year 2018 Internal Audit Work Plan that is acceptable to the Audit and Finance Committee; and

NOW, therefore, it is hereby

RESOLVED, the Audit and Finance Committee of the Board recommends approval of the Internal Audit Work Plan for Fiscal Year 2018 by the Governing Board as presented.

BACKGROUND

The annual internal audit work plan is required by the Tex. Gov't Code §2306.073(b), the Texas Internal Auditing Act (Tex. Gov't Code Chapter 2102) and by the International Standards for the Professional Practice of Internal Auditing (Standards). The plan is prepared by the internal auditor based on an agency-wide risk assessment as well as input from the Department's Governing Board and executive management. The plan identifies the individual audits to be conducted during Fiscal Year 2018. The plan also outlines other planned activities that will be performed by the Internal Audit Division.

Texas Department of Housing and Community Affairs
Office of Internal Audit
Audit Plan for Fiscal Year 2018

Statutory and Professional Standards Requirement

The Texas Internal Auditing Act (Texas Government Code, §2102.005) requires state agencies to conduct a program of internal auditing. The *International Standards for the Professional Practice of Internal Auditing (IA Standards)* define Internal Auditing as an "independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes."

The Texas Government Code and the *IA Standards* require internal auditors to develop an annual audit plan, using risk assessment techniques, that identifies individual audits to be conducted during the year. The Code requires that the plan be approved by the state agency's governing board or by its administrator, if the agency has no governing board.

The program of internal auditing is carried out by the Office of Internal Audit (OIA) which serves at the direction of the Governing Board. The OIA has prepared this audit plan for consideration and approval by the Governing Board.

Development of the Annual Audit Plan

The Fiscal Year 2018 plan is designed to cover areas of highest risk to the State and the agency; however, it does not cover all risks. TDHCA management should utilize internal controls and other appropriate methodologies to mitigate residual risks not covered by the audit plan.

The annual audit plan was developed using a risk based methodology which included:

- Obtaining management's and the Governing Board's perspectives through surveys and discussions.
- Consulting with the State Auditor's Office and other oversight bodies.
- Reviewing prior TDHCA meeting minutes, audit report findings and recommendations, and budgetary information.
- Evaluating information about key agency business areas, processes, and systems.
- Considering input from internal audit staff.

- Utilizing a matrix whereby identified auditable units were ranked according to standard risk factors.

Projects for Fiscal Year 2018 Annual Audit Plan

We have identified the following projects for inclusion in the 2018 Annual Audit Plan. The project numbers are for identification purposes and may not correspond to the order in which the projects are performed. Also included below is a brief description of functions to be reviewed.

New Audit Projects:

1. **HOME (Fund Tracking)**

   The HOME Investment Partnerships Program (HOME Program or HOME) is funded by the U.S. Department of Housing and Urban Development (HUD). HOME formula grants are used to fund a wide range of activities including building, buying, and/or rehabilitation of affordable housing for rent or homeownership. HOME also provides direct rental assistance to low-income-people. It is the largest Federal block grant to state and local governments designed exclusively to create affordable housing for low-income households.

   The fund tracking component of the HOME program rated high on the risk assessment because of staff turnover and a change in the way HUD is requiring tracking/handling of program income, expenditures, etc.

2. **Neighborhood Stabilization Program (Close-out procedures)**

   The Neighborhood Stabilization Program (NSP) is funded by the U.S. Department of Housing and Urban Development (HUD) for the purpose of stabilizing communities that have suffered from foreclosures and abandonment. The program provides funds to purchase foreclosed, vacant or abandoned homes and residential properties, in order to rehabilitate, resell, or redevelop them.

   The NSP rated high on the risk assessment due to its level of complexity of transactions and processes. Also, close-outs on many NSP contract files are beginning.

3. **Loan Servicing Section of the Single Family Operations and Services Division**
   Loan Servicing is responsible for the set up and maintenance of loan records received in connection with a new loan; the day to day servicing functions such as customer service to borrowers and/or authorized representatives of the borrower, providing payoff statements upon request, processing subordination agreement requests, processing payment of various property insurance renewals; perform collection and workout activities for the in-house serviced single family loan portfolio; and annually, process payments for property taxes, completing the escrow analysis process, and the year end process. The section also works in cooperation with other divisions in processing releases of lien for loan payoff funds received by Financial Administration and posting of loan disbursements approved by program and Financial Administration.

   The Loan Servicing Section rated high on the risk assessment and was selected for audit due to the complexity of transactions for various loan programs and various grant requirements.

4. **Emergency Solutions Grant Program**

The Emergency Solutions Grant (ESG) Program is funded by the U.S. Department of Housing and Urban Development (HUD). The program activities include: prevention of homelessness; assistance to homeless through street outreach; emergency homeless shelter improvements, operation help, and provision of essential services; and rapid re-housing.

The ESG program rated high on the risk assessment due to the turnover of half the staff, and new management.

Carry Over Project:

Bond Finance

The Bond Finance Division is primarily responsible for administering the Department's Mortgage Revenue Bond (MRB) program. MRB programs provide below-market interest rate funds for single family homebuyers and multifamily mortgage loans made to qualifying recipients.

The Bond Finance unit rated high on the risk assessment due to its level of complexity of transactions and processes. Additionally, the Bond Finance unit has not been audited within the last three years.

Administrative and Statutory Projects:

- Review of TDHCA compliance with appropriation riders and other requirements of the Government Code
- Annual Audit Plan and reporting
- Annual tracking of the implementation status of prior audit recommendations
- Completion of Peer Review

Consulting Projects and External Audit Coordination

Pursuant to the TDHCA internal audit charter, the OIA performs consulting activities for the agency. For fiscal year 2018, OIA is providing consulting services related to the new Grant Guidance in 2 CFR 200, as well as subrecipient monitoring.

OIA also coordinates and advises on external audit activities.

Sincerely,

Mark Scott, CPA, CIA, CISA, CFE, MBA
Internal Audit Director

MS/BE

REPORT ITEMS

R1

Presentation and discussion of the Report on the Internal Audit "Review of Operations in TDHCA's Information Systems Division"

TEXAS DEPARTMENT OF HOUSING AND COMMUNITY AFFAIRS
An Internal Audit of the Information Systems Divisions (IS)
Audit Report # 17-001

Executive Summary

The Office of Internal Audit (OIA) assessed the TDHCA Information System Division's current compliance with the Texas Administrative Code ("TAC"); reviewed activities of the programmers and technicians; tested appropriate employee access to TDHCA systems; and assessed management and staff time spent on problems with help desk tickets. OIA also observed the areas where the file servers, firewalls, and other network hardware components are deployed. Based on the fieldwork performed, OIA concludes that the Information System Division's functions are generally performed accurately and according to applicable rules; however, the following opportunities for improvement were identified.

Findings and Recommendations

- IS should develop a protocol for testing information systems and designate an individual to be responsible for the internal risk assessment component of the overall governance structure.
- The division should develop and implement a more comprehensive program of IS training for users.

Response:
Management agreed with our recommendations.
Detailed responses are included in the body of the audit report.

Responsible Area:
Information System management

Objective, Scope and Methodology

Based upon our risk assessment and other factors, we selected the Information Systems Division for detailed testing and analytical procedures. This audit was identified in the Fiscal Year 2017 Annual Audit Plan and included the evaluation of the administrative and internal control procedures related to the Information Systems Division.

The current audit covered activities and processes in place during fiscal year 2017. Prior external reviews of IS covered information security and specific program applications. This is the first comprehensive internal audit of IS operations.

_____

Mark Scott, CPA, CIA, CISA, CFE, MBA
Director, Internal Audit

8/24/2017
Date Signed

TEXAS DEPARTMENT OF HOUSING AND COMMUNITY AFFAIRS

www.tdhca.state.tx.us

8/24/2017

Board Members of the Texas Department of Housing and Community Affairs ("TDHCA")

RE: REVIEW OF OPERATIONS IN TDHCA'S INFORMATION SYSTEMS DIVISION

Dear Board Members:

This report presents the results of the Office of Internal Audit ("OIA") *"Review of Operations of TDHCA's Information Systems Division ("IS")."* This audit was identified in the Fiscal Year 2017 Annual Audit Plan. This audit was conducted in accordance with applicable audit standards.

OIA assessed current compliance with the Texas Administrative Code ("TAC"); reviewed activities of the programmers and technicians; tested appropriate employee access to TDHCA systems; and assessed management and staff time spent on problems with help desk tickets. OIA also observed the areas where the file servers, firewalls, and other network hardware components are deployed.

The current audit covered activities and processes in place during fiscal year 2017. Prior external reviews of IS covered information security and specific program applications. This is the first comprehensive internal audit of IS operations.

This report is divided into the following sections:
A. Introduction
B. Governance
C. Components of Information Systems at TDHCA
D. Funding and Staffing
E. Information Systems Compliance
F. Programming
G. Security

A. INTRODUCTION

The Texas Internal Auditing Act requires periodic audits of a state agency's major systems, including major information systems. TDHCA information systems are managed by IS. According to the Director of IS, the division's two major roles are 1) development, implementation, and maintenance of software and 2) technical support with respect to TDHCA employees and the agency's network. As described further below, both of these areas require constant attention to the security of information resources.

In addition to the Internal Audit Act requirement to perform periodic IS audits, the International Professional Practice Framework ("IPPF"), or Red Book (internal audit guidelines), and the Information Systems Audit and Control Association ("ISACA") both require periodic audits of various aspects of IS operations including Governance. IS Governance is generally defined as "the set of decisions rights and the guiding accountability framework designed to ensure that IT resources are employed appropriately in the organization."

B. Governance:

As noted, IS describes its major services as software development and technical support. Statewide direction in these areas is provided by the information technology oversight agency for all state agencies, the Texas Department of Information Resources ("DIR").

State agencies must interact with DIR and implement directives from that oversight agency. DIR conducts periodic "penetration tests" of the networks managed by state agencies. During these tests, DIR attempts to gain unauthorized access to the agency's systems through various methodologies. In the last penetration test of TDHCA systems, DIR was not able to penetrate the network.

Additionally, DIR has a contract with Gartner, a private company that contracts with the state. Gartner provides various security assessment services for state agencies. Gartner conducted a study for TDHCA during FY 2015 and 2016. This study formed a significant part of the basis for TDHCA's FY 2018-2019 Legislative Appropriation Request ("LAR") for strengthening security. The study indicated areas where TDHCA was in need of improvement, and those security areas were factored in to the LAR, with estimates for information technology hardware, software, and services. It is noted that the request did not reflect the full amount Gartner identified as IS prioritized Gartner's recommendations, performed its own assessment of its ability to address the issues identified, and developed effective solutions for a reduced total cost.

One area that needed attention, based both on DIR reviews and the Gartner assessment, concerned "building in" security as applications are developed. Currently IS deals with programming security primarily by after-the-fact "patches" rather than testing programs along the course of production. This area of risk mitigation is becoming increasingly important as hackers develop more sophisticated methods. Industry guidance in this area is provided by the Open Web Application Security Project ("OWASP") and the United States Computer Emergency Readiness Team ("US-CERT") Build Security In ("BSI") web portal.

Finding and Recommendation:
IS should develop a protocol for testing information systems and designate an individual to be responsible for the internal risk assessment component of the overall governance structure.

Finding Item Number	Management Comments – Status Pertaining to the Recommendations and Action to be Taken	Target Completion Date	Responsible Party
17-001.01	Management agrees with the finding and will take actions to improve security testing of information systems. The FY 2018 budget includes funding for a new full-time equivalent position that will be filled early in the fiscal year. That position will be dedicated to security testing and quality assurance of agency software applications. IS will also acquire an internal vulnerability assessment tool and implement a new web application firewall to help protect against common attacks. These actions will complement existing security controls and testing activities, including DIR security scans, periodic Internet-based scans of web application software performed by IS, and multiple firewall layers that are already in place. Regarding the internal risk assessment component of the overall governance structure for information security, TDHCA's Information Security Officer has been designated as the person responsible and now coordinates the security risk assessment process.	December 31, 2017	Information Security Officer

C. COMPONENTS OF INFORMATION SYSTEMS AT TDHCA

The components of TDHCA's overall information systems environment include IS staff, TDHCA staff who are users of the systems, hardware, software, and external users. Information systems are like chains, in that the weakest link determines their strength. The weakest link is often considered to be the users. Users are vulnerable to "social engineering" attacks, whereby hackers alleging a variety of scenarios gain access to information systems. Examples include hackers claiming to be technicians making repairs and requesting confidential information from users to complete the repair.

TDHCA provides security awareness training to employees. Internal audit conducted a customer survey of TDHCA staff, and the result indicated desire for more training. Internal audit recommends a more robust training program for users, instruction on how to use software, and ongoing security training. To provide incentives, evaluations could include the taking of training as a scoring item for evaluations or internally posted jobs.

Finding and Recommendation:
The division should develop and implement a more comprehensive program of IS training for users.

Finding Item Number	Management Comments – Status Pertaining to the Recommendations and Action to be Taken	Target Completion Date	Responsible Party
17-001.02	Management agrees with the finding and will take the following actions to aid agency employees in general IS training and information security training: 1) Provide TDHCA division management with assistance in using training budgets for low cost technical training subscriptions offered through DIR contracts. 2) Improve the existing security training program through a newly acquired web-based training service that will be continuously available to all employees.	October 31, 2017	Information Resources Manager

D. Funding and Staffing

IS received approximately $1.7 million in 2017 and $1.88 million in FY 2018 for operations from a direct appropriation in the TDHCA bill pattern Goal, F.1.2 strategy; Information Resource Technologies. The Division had 20 staff members as of April 20, 2017. Two full-time equivalent positions will be transferred to IS in FY 2018 to assist with the Cybersecurity Initiatives capital budget project, which is the primary reason for the increase in FY 2018.

TDHCA also receives appropriations for capital budget projects. For FY 2017 the capital budget for IS was $189,000. Capital projects may include hardware, software upgrades, and man-hours for internal work to develop software applications and enhancements.

E. Information Systems Compliance

As noted in section B of this report on Governance, parameters for IS compliance are established primarily by DIR and are laid out in 1 TAC Chapter 202.

Exhibit A depicts the division of responsibilities for IS compliance between DIR and TDHCA. The purpose of this area of the audit was to evaluate compliance and recommend improvements. We did not test to an extent so as to determine full legal compliance. The following areas, based on interviews or examination of documents, indicated potential for improvement.
1. Line of Reporting of the Information Security Officer ("ISO")
2. Spanish Language Accessibility
3. Health Insurance Portability and Accountability Act of 1996 ("HIPAA") requirements

Observation:

TAC §202.21 states that the ISO shall report to executive level management. Our review indicated that the ISO has dual reporting relationship; however the organizational chart provided by Human Resources does not show this reporting requirement. IS should revise and update all organizational charts to reflect the reporting requirements per 1 TAC §202.21.

F. Programming

TDHCA has a wide array of funding sources and programs. IS maintains an internal administrative system to manage time-keeping, payroll, and other personnel-related areas. The agency also has a variety of systems for managing funds flow from the state and federal sources. Exhibit B lays out the various information systems used by the agency. This exhibit was prepared by internal audit and IS.

G. Security

Information system security has in recent years and months come to the forefront of concerns related to electronic data. Primary concerns include; 1) e-Commerce vulnerabilities, 2) identity theft, and 3) hacking and other matters related to the security of data that is used in our everyday lives.

1) TDHCA does not conduct e-Commerce. 2) The agency has protocols to protect personal identifying information and other protected or confidential information of employees and other stakeholders. The agency has various transactions with program beneficiaries, subrecipients, and other parties. The agency's various systems interact with the Texas Comptroller of Public Accounts and federal funding agencies. IS has various protocols and controls to protect the identity of these parties. 3) The agency utilizes firewalls and other appropriate anti-hacking protections.

OIA extends our sincere appreciation to management and staff of the Information Systems Division for their cooperation and assistance during the course of this audit.

Sincerely,

Mark Scott, CPA, CIA, CISA, CFE, MBA
Internal Audit Director

MS/BE, NS

cc: [note: lower case]

Exhibit A

SOURCE: Texas Administrative Code ("TAC") Title 1, Part 10, Chapter 202; Texas Government Code Chapter 2054; Texas Department of Information Resources (DIR) website.

PURPOSE: To determine the responsibilities and duties of TDHCA and DIR.

PROCEDURE: Read the TAC and document the responsibilities of TDHCA and DIR.

RESULTS:

Each state agency is ultimately responsible for the agency's information resources. Also, the Executive Director is charged with ensuring that senior management and information-owners, in collaboration with the Director of Information Systems and the Information Security Officer, support the provision of information security for the information systems that support the operations and assets under their direct or indirect control.

Responsibilities Under Texas Administrative Code	
DIR Responsibilities:	**TDHCA Responsibilities:**
General Administration:	Responsibilities of Executive Director ("ED"):
Provide functional support to state agencies	Designate an Information Security Officer ("ISO");
Employ a statewide data coordinator to improve the control and security of information collected by state agencies; promote between state agencies the sharing of information; and reduce information collection costs statewide.	Allocate Resources;
Develop and implement best practices among state agencies.	Ensure that senior agency officials and information-owners support information security and the ISO;
Appoint a customer advisory committee	Ensure that agency has trained personnel to assist in complying with DIR requirements;
Provide the leadership in and coordination of information resources management within state government.	Approve high level risk management decisions
Develop and publish policies, procedures, and standards relating to information resources management by state agencies and ensure compliance	Review and approve at least annually the department information security program; and
Provide and coordinate an information resources management training program for the departments of state government.	Ensure that information security management processes are integrated with department strategic and operational planning processes.
Work with state agencies to ensure deployment of standardized contracts.	Responsibilities of the ISO:
Establish and administer a clearinghouse for information relating to all aspects of protecting the cyber security of state agency information.	Shall report to Executive level management;
Develop strategies and a framework for the securing of cyberinfrastructure by state agencies and cybersecurity risk assessment and mitigation planning.	Has authority for information security for the entire agency;
Adopt rules for digital signatures	Shall possess training and experience required;
Provide mandatory guidelines to state agencies regarding the initial and continuing education requirements needed for information resources managers ("IRM") and require IRMs to report their	Whenever possible, has information security duties as primary duty;

compliance.	
Establish return on investment guidelines to help state agencies to implement major information resources projects more effectively.	Develop and maintain agency-wide security plan, and information security policies and procedures;
Prepare the state strategic plan, in coordination with the quality assurance team and state agency IRMs.	Provide training and direction of information security personnel;
Prepare instructions for use by state agencies in preparing the agency strategic plan.	Provide guidance and assistance to agency personnel;
Review the Information Resources Deployment Review submitted by state agencies	Ensure that annual information security risk assessments are performed and documented by information owners;
Develop and maintain the Cooperative Contracts Program	Review the agency's inventory of information systems and related ownership;
Adopt rules to implement the removal of data from data processing equipment.	Cooperate and coordinate with the agency Information Resources Manager ("IRM"); and
Adopt data use agreement rules that relate to information security standards for state agencies.	Report, at least annually, to the state agency head, the status and effectiveness of security controls, the adequacy and effectiveness of information security policies, procedures, and practices, and compliance with DIR Information Security Standards.
Establish requirements of what is to be included in the Information Security Program.	Information owners, custodians, and users of information resources shall, in consultation with the agency IRM and ISO, be identified, and their responsibilities defined and documented by the agency.
Establish plans and policies for a system of telecommunications services	The agency shall develop, document, and implement an ED approved agency-wide information security program.
Develop a statewide telecommunications operating plan for all state agencies.	Perform and document a risk assessment of the agencies' information and information systems.
Adopt appropriate policies and standards that govern the cost-effective and efficient management, operation, and use of state telecommunications services.	Public solicitation of bids or proposals is required for interagency contracts and the agency must determine whether the bid or proposal meets DIR criteria.
Manage the operations of statewide technology centers that provide data center services or disaster recovery services for two or more state agencies.	Submit Statements of Work, greater than $50,000 to DIR, for Cooperative Contracts Services.
Designate a state cybersecurity coordinator to oversee cybersecurity matters for the state.	Provide written notice to the Legislative Budget Board ("LBB") of a contract for a major information system.
Cybersecurity assessments by Controlled Penetration Testing ("CPT")	All users and developers of geographic datasets and geographic information systems must comply with geographic technical standards
Web Application Vulnerability Scanning ("WAVS")	Make a procured public domain geographic dataset (Federal or other) available to the Texas Natural Resources Information System ("TNRIS").
Open Web Application Security Project ("OWASP")	Unless an exception is approved by the agency head or an exemption has been made for specific technologies, all new or changed web pages must comply with standards and specifications, and be tested.
Web Application Security Consortium ("WASC") standards	A state agency must establish an accessibility policy which must include criteria for monitoring its website for compliance with the standards and specifications.

End-user security awareness training	Make a reasonable effort to ensure that Spanish-speaking persons of limited English proficiency can meaningfully access agency information online.
Monthly webinars are hosted for Security Professionals in the Texas state government system	Protect the privacy and personal identifying information of members of the public who provide or receive information from or through the agency website.
Annual threat report to promote awareness of threat actors targeting state assets	Publish a privacy notice that describes applicable provisions of the privacy policy on the home page and all key public points or the site policies page.
Maintain and post the Security Control Standards Catalog	Prior to providing access to information or services on the website, that requires personal identifying information, conduct a transaction risk assessment, and implement appropriate privacy and security safeguards.
State Website Linking and Privacy Policy	Complete an information resources deployment review.
	Submit an operating plan to the LBB, DIR, the quality assurance team, and the governor each state fiscal biennium.
	Permanently remove data from data processing equipment before disposing of or transferring of equipment.
	Develop a data use agreement related to information security standards for state agencies.

Exhibit B

TDHCA Applications

Application/System Name	Used By or Programs Supported	Description
Enterprise Commercial Off-The-Shelf Systems		
HAPPY Housing Pro (Section 8 System)	Section 8	Community Affairs' Section 8 team uses Housing Pro to administer the Section 8 program. Tenant and payment information is managed in the system and interfaced to PeopleSoft Financials once a month. Housing Pro is a product of HAPPY Software. It is installed in TDHCA's network and administered by the Information Systems Division ("ISD"). Housing Pro is available within the TDHCA network; there are currently no external-facing components.
Microsoft Exchange	Agency-Wide	Microsoft Exchange is the agency's email server software. TDHCA employees can access it internally and externally.
Mitas	Financial Administration, Single Family Operations & Services, and other divisions	The two Mitas systems used by TDHCA are the Mitas Loan Origination & Servicing System and the Mitas Accounting System. Mitas is a product of the Mitas Group, Inc. It is installed in TDHCA's network and administered by the Information Systems Division ("ISD"). The Mitas Loan Origination & Servicing System supports all daily loan origination & servicing processes for the agency's in-house special loan portfolio. Mitas is also used to monitor participating servicers under the whole loan portfolio. Monthly billing statements and borrower credit reporting are also generated by the Mitas system. All loan portfolio year-end reporting, escrow analysis, and disbursement processing for taxes and insurance are generated and managed within the Mitas Loan Origination & Servicing System. One Mitas component, the Bootstrap Loan Reservation System, is available on TDHCA's website and provides Colonia Self-Help Centers and certain nonprofits with the ability to reserve funds for the Texas Bootstrap Loan Program. All other Mitas components are accessible internally only. The Mitas Accounting System provides monitoring and tracking of all investments (i.e.,

Application/System Name	Used By or Programs Supported	Description
		mortgage backed securities and money markets) related to Single Family, Multifamily, and Special Housing Programs and is used to reconcile with trustees. Mitas is also used to perform monthly posting and create ledger detail for agency housing programs. Mitas is used to develop and generate financial statements and quarterly investment financial reports.
PeopleSoft Financials	Financial Administration and Agency-Wide	PeopleSoft Financials is the accounting system of record for governmental funds managed by TDHCA and agency procurement. It is used to perform grants accounting, accounts payable, and general ledger functions, and it interfaces daily with Comptroller's Office systems such as the Uniform Statewide Accounting System ("USAS"). One of the major FY 18-19 capital budget projects involves an upgrade to the latest State of Texas version of PeopleSoft Financials (the Centralized Accounting and Payroll/Personnel System - Financials, or CAPPS Financials) which is distributed by the Comptroller's Office. PeopleSoft Financials is accessible internally only, with the exception of the daily interfaces. In July 2017, TDHCA migrated to the CAPPS Human Resources/Payroll system as a Central Agency, meaning that the Comptroller's Office hosts and administers the system and TDHCA (and other agencies) use the system as a service. TDHCA will be a Hub Agency for CAPPS Financials, which means that the Comptroller's Office will provide the software to TDHCA, and we will install it in our network and add customizations needed for agency housing and community affairs programs.
TeamMate	Compliance and Internal Audit	TeamMate is audit management software. The Compliance Division is the primary user of the software, which provides features for organizing and tracking work papers associated with monitoring visits. ISD supports the installation of the software on agency computers, as well as a TeamMate web and database server. TeamMate is available internally only.
Serv-U	Agency-Wide	Serv-U is secure, web-based file transfer software

Application/System Name	Used By or Programs Supported	Description
		used by many TDHCA divisions for exchanging files with subrecipients and other customers. The software is available internally and externally.
Central Database Suite of Systems (Custom Developed in Java) Note: All Central Database systems are interrelated and share a common database.		
Community Affairs Contract System ("CACS")	Community Affairs and HOME, for administration of: CEAP, CSBG, WAP, ESG, HHSP, and LIHEAP (and historical ARRA contracts)	The two major modules of CACS are the Contract module and the Subrecipient Reporting module. The Contract module allows TDHCA to setup CA contracts and electronically route them for approval, through subrecipients and various TDHCA approval levels. The Subrecipient Reporting module allows subrecipients to submit performance and expenditure reports to TDHCA for approval and processing. CACS is accessible internally and externally.
CSBG National Survey System	Community Affairs	This system is accessed through CACS and provides CA subrecipients with the ability to enter and submit CSBG national survey information to TDHCA. It is available internally and externally. Note: This system was developed in PL/SQL; the other Central Database systems are built in Java.
Compliance Monitoring and Tracking System ("CMTS")	Compliance and Agency-Wide	CMTS allows TDHCA to enter, track and update compliance and monitoring data and other information associated with people, organizations, and properties for multifamily programs, including Housing Tax Credits, Multifamily Bond, and HOME Rental Housing Development. CMTS is accessible internally only; the CMTS Property Reporting System is accessible internally and externally.
CMTS Property Reporting System	Compliance and Property Owners/Managers	This is the external-facing component of CMTS, through which property owners and managers enter and submit household and tenant data and compliance status reports to TDHCA. Properties that have their own, inhouse systems can use the CMTS Unit Upload feature to submit household and tenant data in batch, thereby eliminating the need for dual entry into CMTS.
Housing Contract System ("HCS")	HOME, Multifamily, Single Family Operations & Services, Financial	HCS is composed of two major components: 1) the Fund Allocation module and 2) the Contract module. The Fund Allocation module is responsible for tracking the distribution of funds

Application/System Name	Used By or Programs Supported	Description
	Administration, and the General Land Office, for administration of: HOME, HTF, NSP, TCAP, and CDBG Disaster Recovery (and historical ARRA contracts)	from external sources, such as HUD or General Revenue, to external housing program subrecipients. The Contract module allows TDHCA to setup and manage contracts and contract activities. External contract administrators login to the system to submit contract activities and draws to TDHCA. HCS is accessible internally and externally.
Housing Resource Center Information Clearinghouse ("HRC-IC")	Housing Resource Center, Agency-Wide, and open to all website visitors	HRC-IC is the system name for the Help for Texans search tool located in the upper left of the front page of the TDHCA website. It provides a way for visitors to find organizations in their area (within Texas) that offer financial assistance for home buying, paying rent, or repairing homes. Visitors can also search for vacancies in properties funded through TDHCA and find assistance for utility bill payments and services for homeless persons. HRC-IC is accessible internally and externally.
Manufactured Housing System (Custom Developed in PL/SQL and Java)		
Manufactured Housing ("MH") System	Manufactured Housing	Language: PL/SQL Internal and some external use. The MH System includes several modules used for the administration of the Texas Manufactured Housing Standards Act. Internal modules include Licensing, Consumer Complaints, Tax Liens Statements of Ownership, Cash Receipts, and Installations. External modules include Form T, Tax Lien, Texas Inventory Finance Agreement, and Consumer Complaint forms.
MH Search Our Database (MHWeb)	Manufactured Housing Customers	Language: Java Accessible internally and externally. MHWeb is a read-only system that provides customers with views, reports, and downloads of Licensing, Home Ownership, Installation, and Tax Lien Data captured in the MH System. The system is accessed through the Search Our Database link at http://www.tdhca.state.tx.us/mh/index.htm.

Application/System Name	Used By or Programs Supported	Description
Website and Public Web Applications **(Custom Developed in PL/SQL and Java, and some Commercial Off-The-Shelf)**		
TDHCA Website	Agency-Wide	Language: HTML and JavaScript Accessible internally and externally. The TDHCA website (www.tdhca.state.tx.us) is administered by ISD and contains pages, documents, and other content on agency programs and services. It also serves as the portal for the external-facing web applications described throughout this list.
Affirmative Marketing Tool ("AMT")	Compliance, Agency-Wide, and open to all website visitors (targeted toward property owners)	Language: PL/SQL Accessible internally and externally. AMT is an external web application located on the TDHCA website at http://www.tdhca.state.tx.us/pmcomp/forms.htm that allows website visitors to view demographic data by property or census tract, for the purposes of affirmative fair housing marketing.
Closing Status Database	Fair Housing, Data Management & Reporting ("FHDMR"), HOME, Single Family Operations & Services, and open to all website visitors (targeted toward subrecipients of housing programs)	Language: HTML and JavaScript Accessible internally and externally. The Closing Status Database (located at http://www.tdhca.state.tx.us/closing-status/index.htm) allows website visitors to track the status of their loans associated with TDHCA housing programs. The data displayed is managed internally through an Access database administered by FHDMR.
Intranet HR Schema	Agency-Wide	Language: PL/SQL Accessible internally and externally. ISD manages a process that loads a few fields of employee data from the HR System to this table on the intranet, which is used for the staff phone directory on the intranet and the TDHCA website (link near the bottom of the Contact Us page, http://www.tdhca.state.tx.us/au_offices.htm). The fields, which include name, division, section, and phone number, are all non-sensitive, public data.
My First Texas Home ("MFTH") Information Request	Texas Homeownership and open to all website visitors	Language: Java Accessible internally and externally. Simple online submission form for requesting a MFTH information packet, located at

Application/System Name	Used By or Programs Supported	Description
		http://www.tdhca.state.tx.us/homeownership/ft hb/buyer_reqs_step5.htm.
My First Texas Home Mortgage Qualifier	Texas Homeownership and open to all website visitors	Language: Java Accessible internally and externally. Calculator tool that helps visitors determine if they are eligible for MFTH and what their estimated monthly payments will be based on the price of their home and the interest rate, located at http://www.tdhca.state.tx.us/homeownership/ft hb/prequalify.htm.
Multifamily Housing Preservation Clearinghouse	Multifamily, and open to all website visitors (targeted toward property owners)	Language: PL/SQL Accessible internally and externally. The Multifamily Preservation Clearinghouse (located at https://www.tdhca.state.tx.us/multifamily/preser vation/) is designed to facilitate the preservation of existing affordable and subsidized multifamily rental properties in Texas. It provides multifamily property owners a format to market their properties to prospective buyers interested in maintaining the affordability of a property.
TDHCA Email List	Administered by External Affairs and Information Systems, and open to all website visitors	Accessible internally and externally. The TDHCA Email List is accessed through the Join Our Email List link on the front page of the website. The software used is L-Soft LISTSERV® Maestro. ISD manages the server hardware and software configuration, and External Affairs oversees the process of sending emails to subscribers.
TDHCA Online Forums	Administered by Information Systems, and available to all website visitors (subject to the status of each individual forum)	Accessible internally and externally. TDHCA Online Forums are accessed through the Featured Items section of the front page of the website. ISD manages the Website Toolbox service that powers the forums. ISD sets up forums for varying topics as requested by management.
TDHCA Public Complaints System	Housing Resource Center, other divisions, and open to all website visitors	Language: PL/SQL This system has 1) an external component (located at http://www.tdhca.state.tx.us/complaint.htm) that provides the public with a means to submit complaints to TDHCA and 2) an internal component for tracking the complaints.

Application/System Name	Used By or Programs Supported	Description
Internal Applications (Custom Developed in APPX, Java, and PL/SQL)		
CDBG Contract Tracking System	Single Family Operations & Services	Language: PL/SQL Accessible internally only. This system is used by the Colonia Initiatives section of the Single Family Operations & Services Division to manage information for contracts funded from the Community Development Block Grant ("CDBG").
Compliance Status System ("CSS")	Compliance	Language: PL/SQL Accessible internally only. The Compliance Division uses the Compliance Status System for tracking compliance scores on multifamily properties funded through the Housing Tax Credit program and other programs such as Multifamily Bond. Links in CMTS help Compliance staff navigate to associated data in CSS.
DAFR and Other Comptroller Office Reports	Financial Administration	Language: PL/SQL Accessible internally only. This is a reporting system that downloads Daily Agency Financial Report ("DAFR") files from the Comptroller's Office and presents them in an easy-to-read format that is accessible on the TDHCA Intranet (for Financial Administration staff).
Federal & Legislative Contact System	External Affairs	Language: PL/SQL Accessible internally only. This system is used to maintain legislator and constituent contact information and associated communication. Included modules: - Federal & Legislative Contact System - Legislator Information System - Legislative Reporting System
Human Resources System and Time & Leave System	Human Resources TDHCA Employees	Language: APPX Accessible internally only. These two closely related systems have been used for TDHCA's HR management and timesheet entries for over 20 years. In July 2017, we migrated to the CAPPS HR/Payroll system, which will replace TDHCA's HR System and T&L System after a three month period of parallel entry.
Hotline Database	Texas Homeownership	Language: PL/SQL

Application/System Name	Used By or Programs Supported	Description
		Accessible internally only. The Hotline Database is used by the Texas Homeownership Division to track information requests for homeownership programs.
Inventory System	Financial Administration and Agency-Wide	Language: APPX Accessible internally only. The Inventory System is managed by the Staff Services area of Financial Administration to track agency inventory. Every TDHCA employee has access to view inventory items assigned to them, which are primarily computers and monitors.
Invoice Tracking System	Financial Administration	Language: PL/SQL Accessible internally only. The Invoice Tracking System is used by Financial Administration to enter and view all invoices received by TDHCA.
Public Information Request ("PIR") System	Legal and Agency-Wide	Language: Java Accessible internally only. Legal is the lead division for PIRs, and they enter and assign PIRs using this system. PIR liaisons in each division also log into the system to enter notes and track the status of assigned PIRs through completion.
Records Management System	Financial Administration	Language: PL/SQL Accessible internally only. The Staff Services area of Financial Administration uses the Records Management System to classify and track agency records.
TDHCA Cash Receipts System	Financial Administration	Language: PL/SQL Accessible internally only. Financial Administration records all non-MH cash receipts using this system. (MH cash receipts are recorded in the Cash Receipts module of the MH System.)
Travel System	Financial Administration	Language: APPX Accessible internally only. The Travel System is managed by Financial Administration to track agency travel requests and expenses. Every TDHCA employee has access to submit travel requests, which are routed to their managers for approval, and then to Financial Administration.
Custom Internal Utilities		
IRS-FORM 1099	Financial	Language: PL/SQL

Application/System Name	Used By or Programs Supported	Description
	Administration	Accessible internally only. Financial Administration uses this utility to produce IRS Forms 1099.
IRS 1099 VB application	Financial Administration	Language: Visual Basic Accessible internally only. Financial Administration uses this utility to create the IRSTAX.dbf file for submission to IRS once a year.
SPA VB application	Financial Administration	Language: Visual Basic Accessible internally only. The Staff Services area of Financial Administration uses this utility to download and print State Property Accounting ("SPA") information. SPA is a Comptroller's Office system.
Toshiba Copy	Financial Administration	Language: PL/SQL Accessible internally only. The Staff Services area of Financial Administration uses this utility for recording Toshiba copy machine costs.
ISD Administration and Reporting Applications (Custom Developed)		
RPNET (External)	Information Systems	Language: Microsoft .NET Accessible internally and externally. This application provides the mechanism for PDF report generation for some external-facing systems, primarily for external-facing MH System components.
RPNET (Internal)	Information Systems	Language: Microsoft .NET Accessible internally only. This application provides the mechanism for PDF report generation for some internal systems, primarily for the internal components of the MH System.
TDHCA Intranet User Account Management ("UAM") System	Information Systems	Language: PL/SQL Accessible internally only. ISD uses the UAM System to manage Oracle accounts for TDHCA's PL/SQL applications. Functions include creating accounts, disabling accounts, assigning roles, and resetting passwords.

R2

Status of 2017 Audit Plan

ORAL PRESENTATION

R3

Discussion of Recent External Audit Activity

ORAL PRESENTATION

R4

Status Update of Peer Review

ORAL PRESENTATION