TEXAS DEPARTMENT OF HOUSING AND COMMUNITY AFFAIRS
An Internal Audit of Information Technology General Controls at TDHCA
Audit Report # 22-001

Executive Summary

IT General Controls ("ITGC") are controls that apply to all systems, components, processes, and data for a given information technology environment. The objectives of ITGCs are to ensure the proper development and implementation of applications, as well as the integrity of programs, data files, and computer operations. The most common ITCGs are:

- Logical access controls over infrastructure, applications, and data.
- System development life cycle controls.
- Program change management controls.
- Data center physical security controls.
- System and data backup and recovery controls.
- Computer operation controls.

OIA reviewed the IT General Controls in place at TDHCA and found its processes require improvement to meet the ongoing strategic and operational goals and objectives of the Agency. However, OIA recognizes the unusual nature of the period audited. Starting in March of 2020 when the Pandemic was recognized as a national and state disaster, the ISD has focused primarily on Pandemic-related technology resource support. This effort included: introduction of full remote working capability for all employees; implementing new technology to support a remote work environment; addition of IT support for new and large Programs funded directly by the US Department of Treasury; provision of information resources for several additional staff at TDHCA (because of new federal Programs, the Agency increased in staff size approximately 25% due to temporary staff allocations); and implementation of additional security due to new infrastructure security exposures. These activities together were the highest priority for the ISD and have been fulfilled in the most expedient way possible. The ISD team completed over 21,000 help tickets during FY2021-2022.

Findings and Observations

1. The DIR Telecommunications room housing the networking equipment that provides Internet access to TDHCA/MH and other agencies should be protected from unauthorized physical access.
2. OIA noted that required monitoring of the DCs was not completed over the audit period. Surveillance cameras have not been functional for over a year; the authorized access list to these restricted spaces and resulting activity logs of physical access were not reviewed periodically.
3. Penetration testing by DIR should be scheduled in the near future to provide assurance that current cybersecurity related defenses in place are adequate.
4. Complete user access reviews, including privileged logical access such as administrator and/or physical access to network equipment and critical business application reviews, should be conducted periodically; at least annually.
5. Governance processes such as status and prioritization meetings for the IS Steering Committee and management, as well as policies including those on requesting IS services, should be reviewed and updated for current needs; then adhered to and monitored by management.
6. OIA recommends that the business users and ISD work together to create a technology "road map" to drive continuous improvement to the IT environment.
7. OIA recommends that performance measures for IT activities be defined and reported more widely on a periodic basis, for example to the Executive Team, directors, and the Board.
8. OIA recommends that the structure and management of Help Desk functions be reviewed, documented in SOPs and managed to standards. SOPs should strengthen communication and ensure backup of critical functions.
9. OIA recommends that System Access Request forms be in place for all changes requested to critical systems access. Forms should be updated to bring simplicity to managing the process for both business users and ISD personnel. ISD should consider a technological solution to tracking these requests to completion.
10. To ensure accuracy of capital asset records, OIA recommends that the business users of the process (Staff Services, ISD, and Financial Administration) determine requirements and implement changes to tracking systems as necessary.

Findings and Observations, continued

11. Physical access to TDHCA/MH facilities should be protected by providing changes including new and terminated employees to DPS on a timely basis with appropriate documentation retained.
12. OIA recommends that changes to network software be monitored by management with evidence of periodic review, to manage the impact to the overall environment. Any known user impacts should be communicated at a minimum to the Help Desk to prepare for user questions.
13. OIA recommends that critical information resources updates such as security certificates are managed using a planning tool to ensure availability of those information resources.
14. OIA recommends that data updates are verified by the business user in production with approval evidenced via email in the Track-it system.
15. OIA recommends that the change management process be enhanced by clarifying roles and responsibilities of the ISD and business users in completing program changes.
16. OIA recommends that requests for IS Services are originated by a manager, Director or other appropriate designee to reduce unnecessary IT involvement for business procedural or training issues.
17. OIA recommends that ISD create a process by which unnecessary code can be removed from the user acceptance environment so that it is not inadvertently moved to Production.
18. Information security officer and agency staff responsibilities require fulfillment per Texas Administrative Code 1 TAC 10 Section 202. In order to function as mandated by TAC, ownership of information and systems by the business user areas is essential. Training for the business users will be required to complete risk assessments and implement appropriate security related controls.
19. Required reporting to DIR should be completed timely with appropriate documentation maintained to support the information contained in the reports.
20. ISD should inventory all vendors to determine what monitoring and security agreements are required then obtain the necessary documentation. If SOC reports are used, verification of the independent accounting firm's certification and TDHCA complementing controls should be completed.
21. OIA recommends that all IT related SOPs be reviewed, updated and signed by management for consistency and efficiency of IT operations.

Management Response

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

Objectives, Scope and Methodology

OIA assessed current compliance primarily with the Texas Government Code Chapter 2054 *Information Resources* ("TGC") and Texas Administrative Code 1 Part 10, Chapter 202 *Information Security Standards* ("TAC"); reviewed activities of application programmers and technicians; validated the process of granting and revoking appropriate employee access to TDHCA systems and resources; tested application development and network change management procedures in place; examined inventory procedures; collected and analyzed customer feedback regarding ISD functions from TDHCA and MH internal staff via survey; reviewed current Standard Operating Procedures ("SOP"); evaluated the current vendor management process; and assessed management and staff time spent on problems with help desk tickets. OIA also observed the areas where file servers, firewalls, and other network hardware components are deployed.

Mark Scott

Mark Scott, CPA, CIA, CISA, CFE, MBA
Director, OIA

3/2/2022
Date Signed

TEXAS DEPARTMENT OF HOUSING AND COMMUNITY AFFAIRS

www.tdhca.state.tx.us

Greg Abbott
GOVERNOR

BOARD MEMBERS
Leo Vasquez, *Chair*
Paul A. Braden, *Vice Chair*
Brandon Batch, Member
Kenny Marchant, Member
Ajay Thomas, Member
Sharon Thomason, Member

March 2, 2022

Writer's direct phone # 512.475.3813
Email: mark.scott@tdhca.state.tx.us

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

RE: INTERNAL AUDIT OF THE INFORMATION TECHNOLOGY (IT) GENERAL CONTROLS AT TDHCA

Dear Board Members:

This report presents the results of the Office of Internal Audit ("OIA") "*Audit of the Information Technology (IT) General Controls at TDHCA*". This audit was conducted in accordance with applicable audit standards. IT General Controls rated high on the risk assessment and was included in the approved Fiscal Year 2022 audit work plan. The Division was selected for audit as the Internal Auditing Act requires periodic audits of an agency's information systems. Internal TDHCA Information Systems Division ("ISD") staff deliver TDHCA and Manufactured Housing's ("MH") technology with support from the Department of Information Resources ("DIR").

This report is divided into the following sections:

A. Audit Results
B. Background
C. Physical Security
D. Information Security
E. Governance: Oversight of IT Activities
F. Funding and Staffing
G. Process Review and Testing
    a. Help Desk
    b. Employee Onboarding, Transfer and Termination
    c. Application Program and Network Change Management
    d. Texas Administrative Code (TAC) Review
    e. Required Reporting to DIR
    f. Vendor Management
    g. Standard Operating Procedures
H. User Survey

A. Audit Results

OIA reviewed the IT General Controls in place at TDHCA and found its processes require improvement to meet the ongoing strategic and operational goals and objectives of the Agency. OIA assessed current compliance primarily with the Texas Government Code Chapter 2054 *Information Resources* ("TGC") and Texas Administrative Code 1 Part 10, Chapter 202 *Information Security Standards* ("TAC"); reviewed activities of application programmers and technicians; validated the process of granting and revoking appropriate employee access to TDHCA systems and resources; tested application development and network change management procedures in place; examined inventory procedures; collected and analyzed customer feedback regarding ISD functions from TDHCA and MH internal staff via survey; reviewed current Standard Operating Procedures ("SOP"); evaluated the current vendor management process; and assessed management and staff time spent on problems with help desk tickets. OIA also observed the areas where file servers, firewalls, and other network hardware components are deployed. Further details regarding testing procedures may be found in Section G, Process Review and Testing.

The audit covered activities and processes currently in place and during Fiscal Year 2021. Prior external reviews of IT General Controls during the annual statewide audit covered specific Program (Texas Rent Relief or "TRR") information security and business applications. In addition, OIA completed a review of the Continuity of Operations Plan that included Disaster Recovery testing, a key component of the IT environment, during FY2020.

B. Background

The Texas Internal Auditing Act requires periodic audits of a state agency's major systems, including major information systems. TDHCA and Manufactured Housing (MH) (as well as the General Land Office for Disaster Funds administration) information systems and resources, are managed by the Information Systems Division. The division's major roles are 1) information security and Cybersecurity assessment, monitoring and remediation; 2) development, upgrade, implementation, and maintenance of both software and hardware; 3) compliance reporting to Department of Information Resources and technology project management under Executive governance; and 4) technical support with respect to TDHCA employees and the agency's network. As described further below, all of these areas require constant attention to the security and functioning of information resources. In addition to the Internal Audit Act requirement to perform periodic IT audits, the Institute of Internal Auditors ("IIA") professional practices framework and the Information Systems Audit and Control Association standards require periodic audits of various aspects of IT operations including Governance.

IT General Controls ("ITGC") are controls that apply to all systems, components, processes, and data for a given information technology environment. The objectives of ITGCs are to ensure the proper development and implementation of applications, as well as the integrity of programs, data files, and computer operations. The most common ITCGs are:

- Logical access controls over infrastructure, applications, and data.
- System development life cycle controls.
- Program change management controls.
- Data center physical security controls.
- System and data backup and recovery controls.
- Computer operation controls.

Starting in March of 2020 when the Pandemic was recognized as a national and state disaster, the ISD has focused primarily on Pandemic-related technology resource support. This effort included: introduction of full remote working capability for all employees; implementing new technology to support a remote work environment;

addition of IT support for new and large Programs funded directly by the US Department of Treasury; provision of information resources for several additional staff at TDHCA (because of new federal Programs, the Agency increased in staff size approximately 25% due to temporary staff allocations); and implementation of additional security due to new infrastructure security exposures. These activities together were the highest priority for the ISD and have been fulfilled in the most expedient way possible. The ISD team completed over 21,000 help tickets during FY2021-2022. See ***Appendix A*** for a listing of these projects by category that were also accomplished during the audit period, resulting in the ability of the Agency to meet the challenges presented by new funding and remote work. OIA recognizes that the nature of this time period has been unusual and provides opportunities for lessons learned to strengthen and enhance current processes.

C. Physical Security

Physical access controls over information resources include protecting equipment that resides in a Data Center ("DC") facility from access by unauthorized users and maintaining appropriate environmental controls such as temperature and humidity regulation, alternate power sources for backup purposes, and fire suppression systems. A DC is a repository that houses computing devices like servers, routers, switches, and firewalls along with supporting components like backup equipment and systems necessary for environmental control.

The Department of Information Resources ("DIR") provides TDHCA and MH with its Internet connection; the facility that contains the equipment to provide Internet service for TDHCA and other state agencies is located on the basement level of the TDHCA building (DIR Telecommunications room). TDHCA ISD manages one primary Data Center located in the Rusk building and a secondary DC at TTOC (the building where MH and ISD software development personnel currently reside) along with a workroom on the basement level of the TDHCA building and multiple wiring closets that include networking equipment for different floors of the building.

OIA visited both DCs, the workroom on the basement floor and the DIR Telecommunications room. Based on observation of these physical spaces and discussion with ISD management, OIA found that generally, the TDHCA ISD DCs have appropriate physical access controls in place, with the exception of TTOC requiring additional fire suppression equipment (note that this room now has an electronics safe fire extinguisher as of the date of this report). ISD management began the process of ordering three additional fire extinguishers. Based on our review, OIA found that necessary monitoring was not completed over the audit period.

When OIA visited the DIR Telecommunications room, the door to the repository was wide open and reportedly had been that way for months. There was no surveillance in place, no card key access, and no protection for the networking cables and equipment from unauthorized access from anyone in the building with access to the basement.

Finding Number	Status Pertaining to the Recommendations and Action to be Taken	Target Completion Date	Responsible Party
22-001.01	The DIR Telecommunications room housing the networking equipment that provides Internet access to TDHCA/MH and other agencies should be protected from unauthorized physical access.	NA	Director of Information Systems
22-001.02	OIA noted that required monitoring of the DCs was not completed over the audit period. Surveillance cameras have not been functional for over a year; the authorized access list to these restricted spaces and resulting activity logs of physical access were not reviewed periodically.	3/31/2022	Director of Information Systems

Management Responses

__22-001.01:__ *This network room is outside of TDHCA's control. This room is under DIR's responsibility. TDHCA ISD will contact DIR and begin the conversation of ensuring that the room will be secured.*

__22-001.02:__ *TDHCA ISD is reviewing the current policies and procedures for all auditing activities. TDHCA will complete updating policies and procedures and associated audits.*

D. INFORMATION 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 personally identifiable 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. ISD has various protocols and controls to protect the identity of these parties. 3) The agency utilizes firewalls and other appropriate anti-hacking protections.

Upon request, 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 in 2019, DIR was not able to penetrate the network. However, this testing should be scheduled in the near future as it is required at least biennially.

Finding Number	Status Pertaining to the Recommendations and Action to be Taken	Target Completion Date	Responsible Party
22-001.03	Penetration testing by DIR should be scheduled in the near future to provide assurance that current cybersecurity related defenses in place are adequate.	3/31/2022	Director of Information Systems

Management Response

Although TDHCA ISD did not complete a penetration test of the TDHCA network, TDHCA ISD did complete a penetration test of the Texas Rent Relief program. TRR was a high priority program during this audit period and the internet applications used to administer this program presented a high risk to the agency. TDHCA also successfully completed disaster recovery test exercises during this period as well. TDHCA ISD will request an external penetration test through DIR STS services. TDHCA ISD will try to complete this task as quickly as possible but will be dependent on DIR's scheduling availability. TDHCA ISD will update the appropriate SOPs and associated documentation to ensure this is an annual exercise.

Information security is an ongoing process that requires periodic review of the logical access rights of users to information resources including applications and network structures. (Logical access rights define the ability to perform specific functions within an information system.) Some users are considered "privileged", which means that they have a wider array of access than the average user (for example, Domain Administrator User IDs on the network that allow for deletions or additions; many ISD functions require privileged access). OIA found that there had not been a complete review of user access for critical information resources during the audit period.

OIA noted that FY2022 network user access reviews were completed by the end of the audit reporting period and had been completed for FY2021. Previously, reviews were completed at the network level on a quarterly basis; this review is considered front line in nature and would mitigate most logical access risk. ISD should consider reinstating the practice of these reviews quarterly. In addition, previous internal audits found multiple issues with network folder level access that should be mitigated by a thorough review at folder levels signed off by business users.

Finding Number	Status Pertaining to the Recommendations and Action to be Taken	Target Completion Date	Responsible Party
22-001.04	Complete user access reviews, including privileged logical access such as administrator and/or physical access to network equipment and critical business application reviews, should be conducted periodically; at least annually.	3/31/2022	Director of Information Systems

Management Response

TDHCA ISD will review account audit policy and complete a full account audit review. TDHCA ISD will ensure periodic reviews are performed according to policy in the future.

TDHCA provides security awareness training to employees, contractors and Board members who have access to TDHCA computers and associated networks, at the time of onboarding as well as annually thereafter. A DIR-approved vendor that meets the legislative requirements of House Bill 1118 (87R) and TGC 2054.519 *State Certified Cybersecurity Training Programs*, provides the training; ISD along with Human Resources tracks and assures that training is completed as required, then reported to DIR. OIA reviewed to ensure training was completed and self-reported to DIR by TDHCA for the FY2021 period with no exception noted.

E. Governance: Oversight of IT Activities

The IIA Global Technology Audit Guide 17 *Auditing IT Governance* states that, "Alignment of organizational objectives and IT is more about governance and less about technology. Governance assures alternatives are evaluated, execution is appropriately directed, and risk and performance are monitored."

TDHCA has a wide array of funding sources and programs. ISD 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. In the context of this report, the term "*business users*" means the Administrative and Programs Divisions of the Agency who utilize information resources to meet Agency goals and objectives; they also represent the interests of the external business users.

Prior to the Pandemic and the focus of ISD staff to the immediate needs at that time, the ISD had well documented and generally followed, policies and processes in place for business user prioritization and monitoring of the technology development team's efforts on project deliverables. Since the Pandemic reprioritized efforts to completely new and unplanned projects, many projects either slowed down or stopped entirely. Because the Pandemic efforts took a large percentage of ISD's resources, there was little time for additional communication and coordination between ISD and business divisions.

Previously utilized methods such as SOP 1264.03 Requesting IS Services and the meeting of the IS Steering Team (including quarterly management level meetings to communicate project status) have been successful in providing Governance to IT investments. In addition, an IT "road map" could be helpful in planning ways to reduce complexity of the IT environment (retiring old systems by consolidating into existing, upgrading old infrastructure) while providing additional business functionality.

Performance reporting is a critical aspect of managing any Agency activity so that goals can be set and achieved. Performance measures allow a Division to communicate accomplishments and activities. When performance may fall short, the root causes can be investigated and obstacles removed to reaching goals. Currently the ISD has defined performance measures that are reviewed by its up line Executive management periodically. Some examples of IT activity measurements include system uptime, total number and dollar amount of projects completed, number of employees granted or revoked access, and total problem tickets cleared.

Finding Number	Status Pertaining to the Recommendations and Action to be Taken	Target Completion Date	Responsible Party
22-001.05	Governance processes such as status and prioritization meetings for the IS Steering Committee and management, as well as policies including those on requesting IS services, should be reviewed and updated for current needs; then adhered to and monitored by management.	3/31/2022	Director of Information Systems
22-001.06	OIA recommends that the business users and ISD work together to create a technology "road map" to drive continuous improvement to the IT environment.	8/31/2022	IS Steering Committee

Finding Number	Status Pertaining to the Recommendations and Action to be Taken	Target Completion Date	Responsible Party
22.001-07	OIA recommends that performance measures for IT activities be defined and reported more widely on a periodic basis, for example to the Executive Team, directors, and the Board.	5/31/2022	Director of Information Systems

Management Responses

<u>22-001.05:</u> *TDHCA ISD will review all policies and procedures related to ISSC and SOP 1264.03 Requesting IS Services and route to management for approval.*

<u>22-001.06:</u> *TDHCA ISD will work with business users to gather technology related information from each division. TDHCA ISD will then consolidate this information for ISSC review and prioritization. The final prioritization will be used to produce a technology "road map".*

<u>22-001.07:</u> *TDHCA ISD will create an SOP to govern internal technology related performance measures and route to management for consideration.*

F. FUNDING AND STAFFING

The ISD received funding of approximately $2.0 million in both FY2021 and FY2022 for operations from a direct appropriation in the TDHCA bill pattern Goal, F.1.2 strategy; Information Resource Technologies. The Division is comprised of one Director, two Managers, 19 staff members and 1 Peoplesoft/CAPPS contractor with plans to add 2 additional contractors for capital projects as discussed below; for a total of 25 staff. Among these team members, 11 are dedicated to network and technical support activities (one of whom is designated as Information Security Officer); and 11 to application development. While 4 members of the team (Director of ISD, Software Development Manager, Network and Technical Support Manager, and Information Security Officer) are considered to be management level, they have retained many day to day functions that were inherited from previous positions. This can hamper their ability to elevate to their current positions and to allow for knowledge transfer among the team. This tendency could be related to the relatively new management in place as of this time period; the ISD Director was promoted in August 2019 and the Network and Technical Manager was hired within the audit period. The Pandemic crisis activity was the highest ISD priority as required by Agency needs.

Because of the increase in capital projects and lack of system upgrades historically, the ISD requires additional focus on project management and compliance reporting, as well as communication both internally and externally to business users. OIA noted as well, that over half of the application development programming team is eligible for retirement in the next few years. Based on discussion with management, ISD has started the process of reviewing its organization and determining appropriate needs for the next budget cycle.

TDHCA also receives appropriations for capital budget projects. Capital projects may include hardware, software upgrades, and internal work hours to develop software applications and enhancements. Capital budgets were increased from $880K in FY2021 to $1.5M in FY2022. This increase was primarily due to the addition of the Compliance Management Tracking System (CMTS) upgrade, additional resourcing for Cybersecurity and DIR Shared Technology Services ("STS") data backup and disaster recovery services, DIR STS Office 365, and ongoing upgrades to the TDCHA version of the statewide Peoplesoft/CAPPS system.

Title 9 funding for ISD to support the new federal programs in response to the Pandemic was only recently allowed by the US Treasury. ISD is currently attempting to backfill positions from this funding.

G. Process Review and Testing

Help Desk

The Pandemic presented many challenges to ISD personnel, especially Help Desk. With the advent of remote working, gone were the days of walking to a person's workstation and working with them face to face to solve problems. These issues were compounded by the layers of Internet access and security authorization between all the connection points. Between setting up and onboarding additional employees who were not expected, growth of capital asset procurement, and the difficulties of assisting personnel remotely, the Help Desk managed all these processes with the tools in place, primarily email, Track-It, LogMeIn, and other programs. The environment the Help Desk supports became much more complex as they were required to determine both the Agency setups but what the business users had in place at home.

Despite the issues they faced, the Help Desk and Application Development teams completed over 21,000 help tickets during FY2021-FY2022. (Note that some help activities, where it was a quick phone call or something easy to resolve, are not included in this number.) These help tickets spanned many types of issues and work activities including software, hardware, access to business systems, and sometimes training and consultation. OIA's review found that often there were staff who were contacted directly by others outside ISD to assist with specific issues. Additionally it appeared that the workload was not equitably balanced due to customer preferences for certain personnel as well as subject matter expertise of specific personnel. A common theme found was that there is very little backup support defined within the organization. In addition, it seemed that many personnel looked to leadership to handle problems, as opposed to allowing the Help Desk personnel work through it and learn.

Finding Number	Status Pertaining to the Recommendations and Action to be Taken	Target Completion Date	Responsible Party
22-001.08	OIA recommends that the structure and management of Help Desk functions be reviewed, documented in SOPs and managed to standards. SOPs should strengthen communication and ensure backup of critical functions.	8/31/2022	Director of Information Systems

Management Response

TDHCA ISD management has worked to ensure all primary areas have at least one back up personnel that can function in the event an employee leaves or is unable to perform their assigned job duties. However, due to the size of the team, the multitude of systems we administer and maintain, and previous external and internal audits stressing the importance and need for separation of duties, the performance of the back up in some cases would cause a drop in overall performance. TDHCA ISD management will continue to improve SOPs and associated procedural documentation to improve communication and backup of critical functions.

Employee and Contractor Onboarding, Transfer and Termination

- Logical Access to Information Resources
- Capital Assets Inventory Control
- Physical Access to Facilities

Within the context of this report, the term "*Employees*" means permanent and temporary employees of TDHCA and MH, as well as consultants and contractors who use Agency information resources.

Logical Access to Information Resources

OIA selected a sample of employees and tracked compliance to the process regarding logical access forms, capital assets transfer forms, update of these records to all the required systems, and the logical badge access to building facilities. OIA noted an increase of onboarding from FY2021 to FY2022, in the respect that as of the date of this report, as many employees have been hired to date as the entire past fiscal year. This hiring brought Agency total authorized full-time equivalents ("FTE") (the way the State accounts for number of staff positions) from 313 approved CAP maximum FTEs to 389 that includes temporary FTEs (noting that not all positions are filled).

While testing these employees, OIA noted that there is often excessive coordination back and forth with Division management to define the profiles and access needs of employees. The ISD assists the Divisions to select appropriate access levels; however as business users of these systems, they should understand the underlying security rights granted and how they affect their business processing.

OIA also noted that transferred employees rarely had forms in place for their access updates, and they often were less defined due to the expedited (or uncommunicated) change for these transfers.

Finding Number	Status Pertaining to the Recommendations and Action to be Taken	Target Completion Date	Responsible Party
22-001.09	OIA recommends that System Access Request forms be in place for all changes requested to critical systems access. Forms should be updated to bring simplicity to managing the process for both business users and ISD personnel. ISD should consider a technological solution to tracking these requests to completion.	4/30/2022	Director of Information Systems

Management Response

TDHCA ISD will communicate with the agency to reinforce the current policies and procedures (SOP 1264.01) are known to all agency employees. TDHCA ISD will also strengthen current policies and procedures to cover cross divisional moves of employees to new positions. This will ensure proper termination of system access when an employee's associated job duties change due to moving to a new position.

Capital Assets Inventory Control

When IT capital assets are required for new employees, generally the Division management will discuss these needs with Help Desk personnel. The timing of these requests varies from far ahead of personnel additions to the day ahead of employee start to after the fact. This affects the ability of ISD to manage the process of providing the information resources as required. In addition, OIA found that often the property transfer request currently required to update the property records is sometimes not provided by Division management to Shared Services timely. As a result, underlying records of the capital asset system, Genesis, are inconsistent at a detail level between Divisions and the names associated with equipment is not always updated. Shared Services as well as ISD retains multiple spreadsheets to track these assets.

OIA noted that the current end user hardware vendor, Dell, maintains much of the equipment via long-term warranties; ISD maintains an inventory of parts that are used to upgrade or swap out items that may not be functional. These inventories were observed during the walkthroughs of data centers, work areas and closets.

Finding Number	Status Pertaining to the Recommendations and Action to be Taken	Target Completion Date	Responsible Party
22-001.10	To ensure accuracy of capital asset records, OIA recommends that the business users of the process (Staff Services, ISD, and Financial Administration) determine requirements and implement changes to tracking systems as necessary.	3/31/2022	Director of Information Systems

Management Response

TDHCA ISD and necessary business staff review the ordering and receiving of IT related hardware and software. All equipment is ordered, received, and distributed according to state laws and required procedures. All purchases are approved by ISD, a unique TDHCA inventory number is assigned to the equipment and item placed in inventory. The deployment of inventoried assets includes acknowledgment of receipt and transfer documentation to the employee.

TDHCA ISD, Staff Services, and Financial Administration complete annual reporting of all controlled assets to the Comptroller of Public Accounts ("CPA") through the State Property Accounting ("SPA") system. Staff Services completes an audit of all tracked equipment under TDHCA's control and certifies the results of that audit to CPA. Any missing or unaccounted for equipment must be found or reported as lost or stolen. During FY2021 TDHCA reported that 100% of equipment was accounted for and reported to CPA.

TDHCA ISD will work with Staff Services and Financial Administration to review current policies and procedures and make any improvements that may be necessary.

Physical Access to Facilities

The employee onboarding, transfer and termination process extends to facility badging access that is coordinated through the Staff Services section. Staff Services requests facility access through coordination with the Department of Public Safety that manages badging and parking.

OIA reviewed the underlying documentation for granting and revoking access and found that authorization is not always evidenced, as well as deactivations not occurring consistently when employees terminate. OIA found several employees that had terminated who had not been deactivated during the audit period. In addition, the process of reviewing access periodically is not in place as noted in *Finding 22-001.04*.

Finding Number	Status Pertaining to the Recommendations and Action to be Taken	Target Completion Date	Responsible Party
22-001.11	Physical access to TDHCA/MH facilities should be protected by providing changes including new and terminated employees to DPS on a timely basis with appropriate documentation retained.	3/31/2022	Director of Staff Services

Management Response

TDHCA acknowledges the necessity to promptly deactivate user badges. However, it should be noted that Human Resources recovers all badges from terminated employees on the last day of employment and are no longer in the former employee's possession. This means that although the badge remained active, the former employee had no access to the badge and therefore had no access to TDHCA/MH buildings. TDHCA will strengthen current policies and procedures as noted in this finding.

Application Program and Network Change Management

Change management is the process by which changes to information resources are identified, defined, designed, coded, tested, communicated and implemented. Changes to software may include:

- Network software "patches" or updates required for security or operating systems functionality
- Network infrastructure (hardware) upgrades
- Data updates requested by business users to "fix" input or setup problems
- Business functionality changes driven by new or existing Program needs

OIA noted that the Applications Development Manager was in the process of restructuring and updating the Change Management process policy and procedure. ISD is reviewing a software package that has been in the budget for two years, to better control and document authorizations from appropriate parties for the change management process. This software, called JIRA, is DIR-approved and would manage all changes including Help Desk tickets.

During the FY2021-2022 time frame, the Application Development team completed over 1,000 work orders which included software development and maintenance, reporting, and database updates. During that time frame, OIA found approximately 200 network changes documented in the "IS System Changes" email account in Outlook.

Changes to Network Software

The current SOP and underlying process for network software updates outlines the documentation of the testing and release of these changes into the production environment. It does not currently require explicit management approval for these changes. At times, when the changes are larger and may affect how the user interacts with the information resource, a communication will be sent ahead of the implementation. While it may not be practical to have management review each change, there should be a checkpoint review periodically.

In addition, during the audit period there was a production issue where a security certificate had not been renewed timely, although the ISD already had purchased the renewal. This caused service interruption to both internal and external parties.

Finding Number	Status Pertaining to the Recommendations and Action to be Taken	Target Completion Date	Responsible Party
22-001.12	OIA recommends that changes to network software be monitored by management with evidence of periodic review, to manage the impact to the overall environment. Any known user impacts should be communicated at a minimum to the Help Desk to prepare for user questions.	3/31/2022	Director of Information Systems
22-001.13	OIA recommends that critical information resources updates such as security certificates are managed using a planning tool to ensure availability of those information resources.	3/31/2022	Director of Information Systems

Management Response

<u>22-001.12:</u> *TDHCA ISD will review current SOPs for management review of network changes. THDCA ISD management and employees are in constant communication about network related changes. With only four members (IS Director, Network Manager, ISO, and Network Specialist) being able to make changes explicit management approval seems redundant and may add additional burdens on staff. As noted earlier in this report, three of the four positions listed are management level positions (as noted in F. Funding and Staffing, page 7). At no time during this audit period was a network change made that the ISD Director and Network Manager were unaware.*

<u>22-001.13:</u> *TDHCA ISD will update the necessary SOPs and create necessary documentation to govern the management of all security certificates.*

Business Application Data Changes

Data changes are typically requested from the ISD via a Help Desk request or phone call that is converted to a Track-it ticket (Track-it is the system utilized by ISD to track a problem or activity through to resolution). Once engaged, the application programmer will determine what is required to fix the problem, run the update in a test environment then the Database Administrator will promote the update to production.

Currently, the process does not require user approval to be documented in the Track-it database; several of the tested tickets only had ISD manager approval. In addition, the user did not consistently document their verification of the data update. OIA did note that over the year, when recurring data fixes were required, ISD took action to create online processes for business users to make updates rather than having continuous updates required directly by ISD.

Finding Number	Status Pertaining to the Recommendations and Action to be Taken	Target Completion Date	Responsible Party
22-001.14	OIA recommends that data updates are verified by the business user in production with approval evidenced via email in the Track-it system.	4/30/2022	Director of Information Systems

Management Response

TDHCA ISD will strengthen current change management procedures to ensure user verification is documented. Although not always evidenced by documentation the users with the appropriate authority always requested the change and reviewed the work.

Business Functionality Changes

Business functionality changes implemented in the TDHCA/MH systems environment should follow the Systems Development Life Cycle (SDLC). In this project management process, there are roles and responsibilities that require clarity between the business users and IT functions. Typically, the business users define the need and request IS services; once ISD is able to size the project, it should be prioritized against projects competing for those resources; once prioritized, the business users further detail the requirements of the functionality to be developed which should refine the project estimate; ISD designs and codes the program changes desired, tests the code and promotes it to the user acceptance test environment. At this level, business user testing commences with focus on changes and ensuring other parts of the system maintain proper functionality. When business user testing is complete, the program changes are promoted into the production environment where everyday business processing takes place.

Currently, ISD is often writing combined business and technical requirements for systems changes. This creates a situation where these important roles are merged, and outcomes can be affected by a lack of understanding of the entire business process flow and impacts. In addition, when the business users are more heavily involved, they better understand the functionality being built, can update their SOP accordingly, and can provide training to others in the Division.

Finding Number	Status Pertaining to the Recommendations and Action to be Taken	Target Completion Date	Responsible Party
22-001.15	OIA recommends that the change management process be enhanced by clarifying roles and responsibilities of the ISD and business users in completing program changes.	6/30/2022	Director of Information Systems

Management Response

TDHCA ISD is in the process of updating change management processes and will incorporate a review of these recommendations. TDHCA ISD agrees that business user involvement is key to the successful completion of software development projects.

During the testing of program changes, OIA noted a difference in the process between TDHCA and MH in that the MH Division requires that any request for IS services is originated by a manager, Director, or their designee. TDHCA requests can come from any level of staff; unfortunately these are often training or procedural issues that could be managed within the originating Division.

Finding Number	Status Pertaining to the Recommendations and Action to be Taken	Target Completion Date	Responsible Party
22-001.16	OIA recommends that requests for IS Services are originated by a manager, Director or other appropriate designee to reduce unnecessary IT involvement for business procedural or training issues.	5/30/2022	Director of Information Systems

Management Response

TDHCA ISD acknowledges the recommendation of OIA. TDHCA ISD will seek executive leadership guidance to determine if changes to current procedures are beneficial for TDHCA.

There are times when business functionality software is coded and provided to the business user, however due to needs changing or other reasons, the project or code is no longer needed or desired. During testing of the program changes and discussion with ISD staff, OIA determined that there is no rollback procedure currently in place to segregate the unnecessary code and remove it from the user acceptance environment.

Finding Number	Status Pertaining to the Recommendations and Action to be Taken	Target Completion Date	Responsible Party
22-001.17	OIA recommends that ISD create a process by which unnecessary code can be removed from the user acceptance environment so that it is not inadvertently moved to Production.	Completed	Director of Information Systems

Management Response

TDHCA ISD management has discussed and implemented procedural changes in the aftermath of this event. The changes will ensure that code will not be inadvertently promoted to production in the future.

Texas Administrative Code 1 Title 10 Section 202 Review

State agencies must interact with DIR and implement directives from that oversight agency. Parameters for IS compliance are established primarily by DIR and are laid out in 1 TAC 10 Chapter 202. 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 area regarding the Information Security Officer function, based on interviews or examination of documents, indicated potential for improvement. See ***Appendix B*** for 1 TAC 10 202 excerpts and current status.

Finding Number	Status Pertaining to the Recommendations and Action to be Taken	Target Completion Date	Responsible Party
22-001.18	The Director of Information Systems, Information security officer and agency staff responsibilities require fulfillment per Texas Administrative Code 1 TAC 10 Section 202. In order to function as mandated by TAC, ownership of information and systems by the business user areas is essential. Training for the business users will be required to complete risk assessments and implement appropriate security related controls.	6/30/2022	Director of Information Systems

Management Response

TDHCA ISD will work with business users to complete all required risk assessments.

Required Reporting to DIR

OIA reviewed reporting requirements of state agencies to DIR and found that some reporting was not completed by TDHCA or not submitted timely; these reports are due in even-numbered years:

1. Vulnerability Report – June 15th
2. Information Security Assessment – November 15th
3. IT Infrastructure Report – November 15th

OIA noted that the FY2021 Information Security Plan was submitted after notification from DIR.

Finding Number	Status Pertaining to the Recommendations and Action to be Taken	Target Completion Date	Responsible Party
22-001.19	Required reporting to DIR should be completed timely with appropriate documentation maintained to support the information contained in the reports.	Complete	Director of Information Systems

Management Response

Due to COVID related demands and changes in leadership, although not completed in a timely fashion they have been completed.

Vendor Management

Both the TDHCA business users and ISD utilize various information resources provided by external vendors. The Texas Procurement and Contract Management guide outlines guidance for properly monitoring vendor contracts, which includes progress reports, status reports, financial reports and onsite monitoring. ISD receives various types of reporting from their vendors, however there is no onsite monitoring in place. In lieu of onsite monitoring, ISD may be able to accept an independent auditor's Service Organization Controls (SOC) report that attests to the vendor's internal controls that affect its ability to provide certain services. SOC reports should be evaluated to assure that required internal controls are in place on TDHCA's side that allow reliance on the vendor's internal controls. Note that the independent accounting firm should be verified via the Texas State Board of Public Accountancy website to ensure they are certified. Additionally, some vendors should be required to sign TDHCA's Information Security and Privacy Agreement (ISPA).

During review of the vendor agreements and monitoring, OIA noted very few existing signed ISPAs and SOC reports or other monitoring procedures. Some newer contracts had these documents in place, however it did not appear that all vendors who should have these requirements had fulfilled them.

Finding Number	Status Pertaining to the Recommendations and Action to be Taken	Target Completion Date	Responsible Party
22-001.20	ISD should inventory all vendors to determine what monitoring and security agreements are required then obtain the necessary documentation. If SOC reports are used, verification of the independent accounting firm's certification and TDHCA complementing controls should be completed.	4/30/2022	Director of Information Systems

Management Response

TDHCA ISD is currently working to update all vendor management SOP's and associated procedural documentation.

Standard Operating Procedures (SOP)

An SOP is a procedure specific to the operation of a division that describes the activities necessary to complete tasks in accordance with applicable rules and regulations. It defines expected practices in a process where quality standards exist. SOPs play an important role in any organization and division. They are policies, procedures and standards needed to operate in a successful way. They can create efficiencies, consistency and reliability, fewer errors, and add value to the Division.

OIA reviewed the Level One and Level Two SOP currently in place to manage Information Technology resources. While much of the content still applies to current processes, many of the SOP documents were outdated and several had been signed by previous Executive Directors. The oldest Level One SOP was dated in 2009; the most recently updated was a Level Two SOP completed in 2019.

Finding Number	Status Pertaining to the Recommendations and Action to be Taken	Target Completion Date	Responsible Party
22-001.21	OIA recommends that all IT related SOPs be reviewed, updated and signed by management for consistency and efficiency of IT operations.	8/31/2022	Director of Information Systems

Management Response

TDHCA ISD will review and update all SOPs. In the future, TDHCA ISD will review all SOPs periodically, but not less than annually.

H. User Survey

Internal audit conducted a customer survey of TDHCA and MH staff, and the result indicated a decrease in customer satisfaction in IT services from the initial survey in 2017 to present. Overall, customers indicated a weighted average score for overall satisfaction with IT services of 2.7 as of 2022, compared to a weighted average satisfaction score of 3.2 in 2017. The largest differences in the survey related to Help Desk and Communication. The survey results independently validate the findings included in this report in many instances. OIA will share details with management for further action.

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

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

MS/SN

Appendix A

IT Project Accomplishments
FY2021-FY2022

Type of Project	*Name of Project*	*Business Purpose*
Security Enhancements	Multifactor Authentication	Strengthens information security by requiring both a password and authentication code for login.
	Migration from Windows 7 to Windows 10	Remediated potential security issues with replacement of outdated Windows environment.
	Attivo Networks Active Directory Implementation	Provides capability of auditing network platform to help track and monitor for vulnerabilities, malicious actions, and configuration flaws throughout the network.
	Cybersecurity and Infrastructure Security Agency (CISA) Agreement	Implemented agreement with CISA for continual ongoing external vulnerability scans and reporting for the TDHCA network.
Remote Work Requirement	Microsoft Office 365 Migration	Greatly enhances business continuity to TDHCA and MH staff by allowing for access to emails and other resources from the cloud based system.
	Creation and Support of the Remote Work Environment	Implemented LogMeIn, Global Protect, additional Internet capacity; continues to support a hybrid work environment.
	CISCO Jabber Access	Addition to the phone technology at TDHCA, this allows for desk phone access by TDHCA staff via the internet. Required for remote work answering general line phone calls.
Application Development/ Enhancements for New Programs	Community Affairs New Programs and Reporting	Implemented several new programs, integrated LIHEAP performance measures and other reports.
	Housing Contract System Updates	Added new Programs for 2022/2023, created new CDBG Cares System, added new Amy Young State Wide Admin and Reservation Project funds to Housing Trust Fund.
	Texas Rent Relief Program Utility Provider Information System	Collects information from Texas Utility providers for the purpose of making payments on behalf of program beneficiaries.
	Texas Rent Relief and Homeowner Assistance Fund Coordination	Assisted in evaluation and selection of all vendors; provided IT related support ongoing and via weekly calls with management.

IT Project Accomplishments FY2021-FY2022

Type of Project	*Name of Project*	*Business Purpose*
Legacy Upgrade	Software and Firmware Upgrades for all TDHCA Networking Equipment	Upgraded old technology and increased security by including security appliances and firewalls.
Compliance	Migrant Labor Housing Facility System	Automation of an existing Excel application to handle critical business functions for licensing/inspections of migrant labor housing
	Manufactured Housing Complaint Module	Allows for submission of online web complaints from external homeowners or customer for MH.
	MH Home Maintenance Module	Created to reduce number of data update requests needed for correcting home records.
	Vacancy Clearinghouse Audit Update	Added accessibility to our vacancy clearinghouse.
	HUD LIHTC Tenant File Upload	Created files required by HUD for reporting.
	IRS1099 MISC Filing System	Converted old technology and allowed for direct upload by external parties.
Business Continuity	Disaster Recovery	Successfully completed Disaster Recovery exercise with DIR to validate consistency and integrity of backup data.
Automation	Emergency Solution Grants System	Automation of an existing Excel application to handle critical business functions for Emergency Solutions Grants.
	Community Affairs Household Module	Automation of existing process to allow CA sub recipients to upload files for performance reporting to HUD. Includes LIHEAP, WAP and CSBG.
	Section 811 Project Rental Assistance Upgrade	A complete revamping of the system used to manage the participant application function within the Program.
Annual Systems Maintenance Requirements	Changes required every year for Programs processing and compliance	Requires IT driven updates to critical systems used by TDHCA and MH such as uploading data files, adding new funds and new programs for the coming fiscal year, and reporting.

Appendix B

Development Status of 10 TAC 202 Compliance

The purpose of this Exhibit is to highlight at a summary level, the status of development of processes and policy to meet the requirements of 10 TAC 202, *Information Security Standards*.

TAC 202 Sections		**Current Status**
202.20	Responsibilities of the Agency Head	In place
202.21	Responsibilities of the Information Owner	Assignment of Information Owners and Custodians pending; developing
202.22	Staff Responsibilities	Developing
202.23	Security Reporting	Developing
202.24	Agency Information Security Program	Developing
202.25	Managing Security Risks	Risk assessments pending; developing
202.26	Security Controls Standard Catalog	Developing