Lisa R. Collier, CPA, CFE, CIDA
State Auditor

An Audit Report on

The Information Management Protecting Adults and Children in Texas (IMPACT) System at the Department of Family and Protective Services

December 2021

Report No. 22-011

An Audit Report on

The Information Management Protecting Adults and Children in Texas (IMPACT) System at the Department of Family and Protective Services

SAO Report No. 22-011
December 2021

Overall Conclusion

The Department of Family and Protective Services (Department) has processes and controls related to its Information Management Protecting Adults and Children in Texas (IMPACT) system to help ensure that (1) access to the system is appropriately assigned and (2) data in the system is secure.

However, the Department should strengthen its user access controls and some of its data security practices, and it should ensure that it complies with its policies. Specifically:

- The Department should follow its policies relating to its routing and approval process to request high-level access for its network domain, servers, and IMPACT database.
- The Department should disable user access when it is no longer required and perform annual renewal background checks on external users.
- The Department should consistently implement controls to ensure that either the same individual does not close and approve case stages in IMPACT, or that it was appropriate for the same individual to close and approve case stages in IMPACT.
- The Department established a change management process and Change Approval Board (Board) for evaluating, approving, and implementing changes to IMPACT; however, the Department should improve its documentation of the Board's IMPACT change approvals.
- The Department did not consistently comply with its policies to form and approve agreements with external parties for data exchanges with IMPACT and access to IMPACT.

Background Information

The Information Management Protecting Adults and Children in Texas (IMPACT) system is the official case management system for the Department. IMPACT is a browser-based system that records investigations, case management activities, and services provided by the Department's programs: Statewide Intake, Child Protective Investigations, Child Protective Services, Adult Protective Services, Child Care Investigations, and Prevention and Early Intervention. IMPACT also has a financial module that the Department uses to process payments.

As of April 8, 2021, IMPACT had 12,145 internal users and 1,838 external users. Internal users are Department employees; external users include contractors and users from other agencies. In addition, 13 external agencies and organizations exchange data with the Department through IMPACT.

See Chapter 1 for more information about IMPACT.

Source: Information provided by the Department.

This audit was conducted in accordance with Texas Government Code, Sections 321.0133 and 321.0134.

For more information regarding this report, please contact Michael Simon, Audit Manager, or Lisa Collier, State Auditor, at (512) 936-9500.

- The Department should ensure that it retains supporting documentation to show supervisor approval for all cases deleted from IMPACT.

Table 1 presents a summary of the findings in this report and the related issue ratings. (See Appendix 2 for more information about the issue rating classifications and descriptions.)

Table 1

Summary of Chapters/Subchapters and Related Issue Ratings		
Chapter/ Subchapter	**Title**	**Issue Rating [a]**
1	Background Information on IMPACT	Not Rated
2	The Department Appropriately Assigned High-Level Access to Its Network, Servers, and IMPACT Database; However, It Should Ensure That It Follows Its Policies When Users Request Access	Medium
3	The Department Did Not Consistently Follow Its Policies for Managing User Access to IMPACT	High
4	The Department Did Not Consistently Implement Segregation of Duties in IMPACT	Priority
5-A	The Department Appropriately Documented Business Need and Justification for Changes to IMPACT, But It Should Improve Documentation of IMPACT Change Approvals	Medium
5-B	The Department's Agreements With External Parties Helped Ensure That IMPACT Data Is Protected; However, the Department Did Not Consistently Comply With Its Policies to Form and Approve the Agreements	Low
5-C	The Department Complied With Its Procedures for Deleting Cases from IMPACT, But It Should Ensure That It Retains Documentation to Support Approval of Deletions	Low
5-D	Automated Controls Protect Data in IMPACT	Low

[a] A chapter/subchapter is rated **Priority** if the issues identified present risks or effects that if not addressed could critically affect the audited entity's ability to effectively administer the program(s)/function(s) audited. Immediate action is required to address the noted concern and reduce risks to the audited entity.

A chapter/subchapter is rated **High** if the issues identified present risks or effects that if not addressed could substantially affect the audited entity's ability to effectively administer the program(s)/function(s) audited. Prompt action is essential to address the noted concern and reduce risks to the audited entity.

A chapter/subchapter is rated **Medium** if the issues identified present risks or effects that if not addressed could moderately affect the audited entity's ability to effectively administer the program(s)/function(s) audited. Action is needed to address the noted concern and reduce risks to a more desirable level.

A chapter/subchapter is rated **Low** if the audit identified strengths that support the audited entity's ability to administer the program(s)/function(s) audited or the issues identified do not present significant risks or effects that would negatively affect the audited entity's ability to effectively administer the program(s)/function(s) audited.

Auditors communicated details about issues relating to security risks directly to the Department's management in writing. Auditors also communicated other, less significant issues separately in writing to Department management.

Summary of Management's Response

At the end of certain chapters in this report, auditors made recommendations to address the issues identified during this audit. The Department's detailed responses are presented immediately following each set of recommendations. The Department agreed with all of the recommendations in the report.

Audit Objectives and Scope

The objectives of this audit were to determine whether the Department has processes and controls related to the IMPACT system to ensure that (1) access to the system is appropriately managed and (2) there are key controls to secure and protect the data in the system and these controls are working as intended.

The scope of this audit covered the Department's processes and controls related to user access and data security for the IMPACT system from September 1, 2019, through April 8, 2021. The scope also included a review of significant internal control components related to user access and data security.

Contents

Detailed Results

Appendices

Detailed Results

Chapter 1
Background Information on IMPACT

The Department of Family and Protective Services (Department) began using its original case management system, called Child and Adult Protective Services (CAPS), in 1996. CAPS was transformed into the Information Management Protecting Adults and Children in Texas (IMPACT) system in 2003. The Department modernized components of the system between 2014 and 2019, but some Department programs still use the legacy version of IMPACT to perform certain functions.

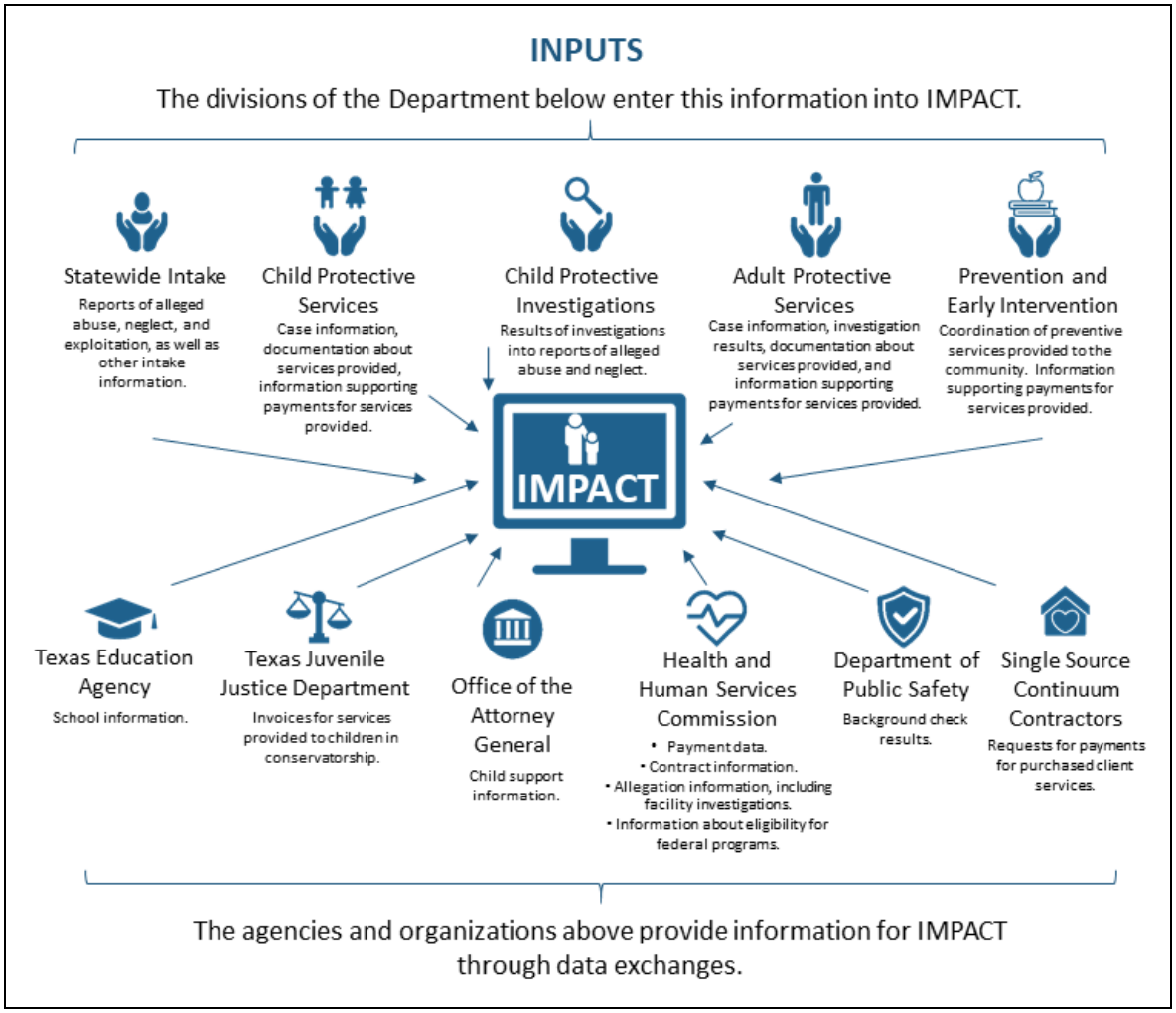
IMPACT Inputs and Outputs

The Department uses IMPACT to document all stages of a case, beginning with intake of a report of alleged abuse, neglect, or exploitation, through investigation and services, to disposition and closure. As a result, IMPACT contains personally identifiable information about victims of abuse, neglect, or exploitation, and about people associated with their cases. The Department uses IMPACT's financial module to process payments to service providers and for program-related payments, such as foster care maintenance payments. Department staff can access data from IMPACT by directly using the system or by reviewing reports that are created from extracts of IMPACT data that are available on the Department's intranet.

In addition to the Department's direct input into IMPACT and output from IMPACT related to its program activities, the Department works with 13 other agencies and organizations to update and share information in IMPACT through automated data exchanges.

Figure 1 on the next page shows a high-level view of the inputs into IMPACT from within the Department and from external agencies and organizations.

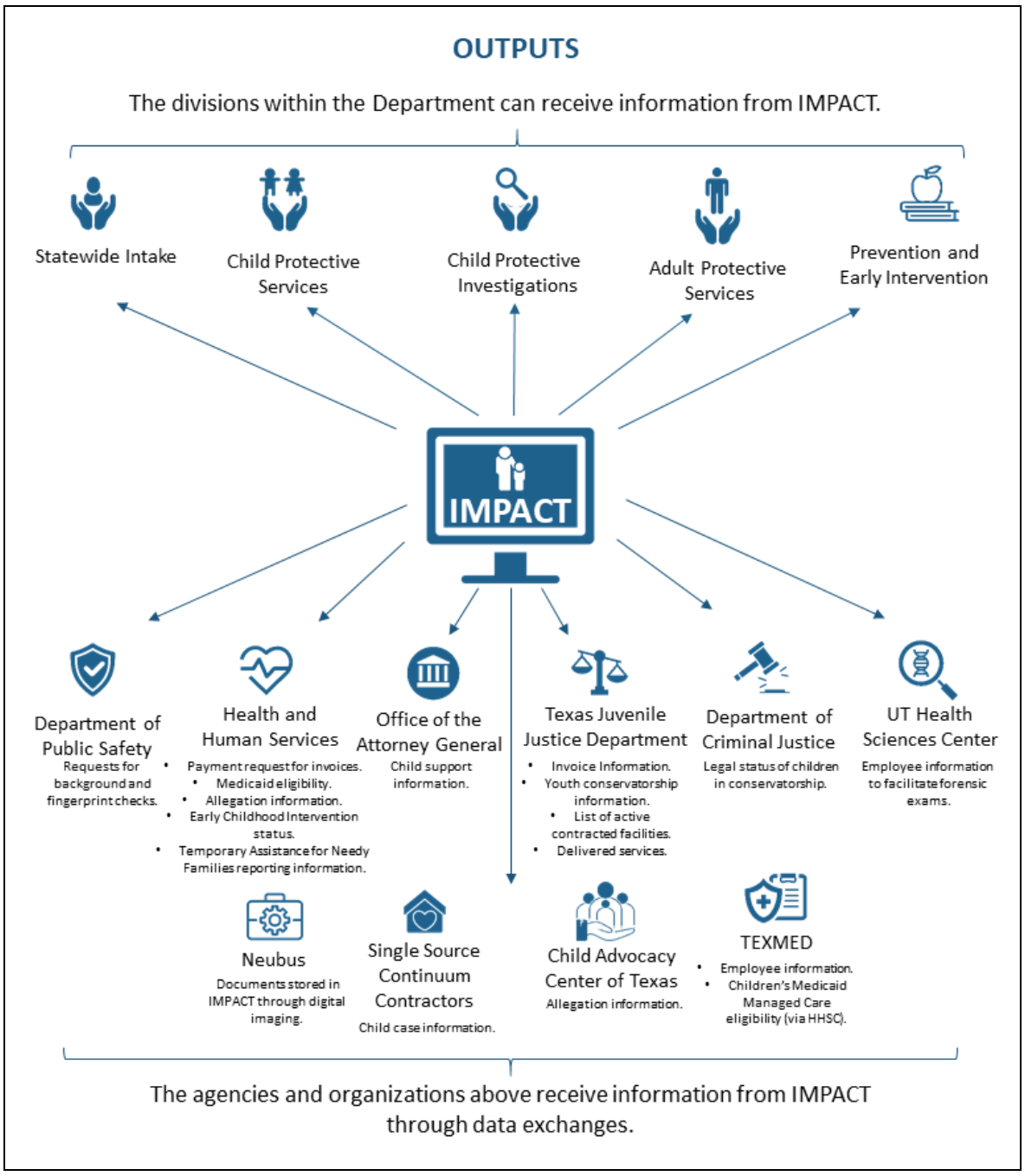
Figure 1



Source: Information provided by the Department.

Figure 2 shows a high-level view of the outputs from IMPACT to divisions within the Department and to external agencies and organizations.

Figure 2



Source: Information provided by the Department.

User Access to IMPACT

Each user accesses IMPACT through their network account. The Department also assigns high-level access to users of the IMPACT database and servers. See Chapter 2 for more information about high-level access.

The Department assigns each user a basic profile in IMPACT that enables the user to perform functions related to the user's position, job duties, regional location, and program. For example, a basic profile for a Child Protective Services investigator provides that user the ability to document regular investigation case information in IMPACT. If the caseworker's job duties also required the ability to work in cases designated as sensitive, the Department would also assign that user an IMPACT security profile to access sensitive cases, in addition to the user's basic profile. Depending on the user's role, the Department may assign an individual user multiple security profiles in IMPACT. See Chapter 3 for more information about security profiles.

As of April 8, 2021, the Department had assigned 33,369 security profiles in IMPACT to 13,983 internal and external users (see Table 2 for a breakdown).

Table 2

Breakdown of IMPACT Users as of April 8, 2021		
Type of IMPACT User	Number of Users	Number of Security Profiles [a]
Internal (Department employees)	12,145	29,037
External (contractors and employees from other agencies)	1,838	4,332
Totals	**13,983**	**33,369**

[a] The Department may assign an individual user multiple security profiles in IMPACT based on the user's position, job duties, regional location, and program.

Sources: User list extracted from IMPACT and information provided by the Department.

The Department's policies require potential users of its network, databases, servers, and individual systems, such as IMPACT, to request access through its routing and approval process.

Chapter 2

The Department Appropriately Assigned High-Level Access to Its Network, Servers, and IMPACT Database; However, It Should Ensure That It Follows Its Policies When Users Request Access

Chapter 2 Rating:

Medium[1]

The Department provided appropriate high-level access to its network domain, servers, and IMPACT database, based on the positions, job duties, and responsibilities of the users tested. However, the Department's process for managing requests for high-level access did not always operate in accordance with Department policies.

Electronic Move, Add, and Change (eMAC) Request System

The eMAC system is the Department's online tool for submitting, tracking, and processing system access requests. The Department uses eMAC to request new employee accounts, equipment assignments, and access to its systems. The requestor submits an eMAC form and Department staff will assign and route the request to the appropriate approval authorities based on the nature of the request. The eMAC form includes sections for the submitter to document the business justification and specific system access rights being requested.

Source: The Department.

The Department implemented policies and controls that require system users to submit documented request forms through its electronic Move, Add, and Change (eMAC) routing system to request access (see text box). The Department also provided guidelines to its staff about how to complete eMAC request forms.

For 3 (30 percent) of 10 users tested, the Department's eMAC routing and approval process did not operate effectively to ensure that all information needed to set up the users' access was included on the forms. For example, the eMAC forms for two of the users included information about granting server access, but did not specify the IMPACT servers.

Lack of documentation of the specific access requested and lack of an effective review and approval process could result in a user being granted inappropriate access.

Recommendation

The Department should follow its eMAC review and approval policies to ensure that the eMAC form includes all information relating to the access level being requested.

[1] The risk related to the issues discussed in Chapter 2 is rated as Medium because they present risks or effects that if not addressed could moderately affect the audited entity's ability to effectively administer the program(s)/function(s) audited. Action is needed to address the noted concern(s) and reduce risks to a more desirable level.

Management's Response

DFPS recognizes that it should review accounts with elevated access to ensure compliance with stated review and approval policies. Management is responsible for reviewing and granting elevated access to staff and will define and document processes to ensure elevated access is reviewed regularly.

Responsible Person, Title: *Interim IT Operations Director*

Implementation Date: *January 31, 2022*

Chapter 3

The Department Did Not Consistently Follow Its Policies for Managing User Access to IMPACT

Chapter 3 Rating:

High[2]

The Department's policies and controls for managing access to IMPACT included approving access (see Chapter 2), assigning users basic access and security profiles based on their duties (see Chapter 1), performing background checks, and conducting annual user access reviews. However, the Department did not consistently disable user access, conduct annual user access reviews, or perform renewal background checks for external users in accordance with its policies.

The Department should improve its controls to disable user access to IMPACT within the required timeframes.

The Department removed access to IMPACT for 40 (89 percent) of 45 employees and 1 (50 percent) of 2 external users who were no longer working with the Department as of April 8, 2021. However, that access was not removed as quickly as required by the Department's policies. Specifically, the Department did not disable the network access for up to 35 days after the employees stopped working with the Department or for 71 days after the external user stopped working with the Department. The Department's policies require that user accounts be disabled within one day of when the user stops working with the Department or after a period of inactivity (see next section). Not removing user and network accounts in accordance with policies could give former employees and external users an opportunity to access data in IMPACT.

In 2018, the State Auditor's Office conducted an audit and identified weaknesses in disabling accounts when employees separate from the Department and in monitoring access of external users to ensure that accounts are disabled when that access is no longer needed.[3]

The Department did not follow its policies to disable access for current users after a period of inactivity.

The Department policy stated the Department is to disable IMPACT access for users who have not logged into IMPACT for 30 days. The Department did not comply with this policy for 65 (54 percent) of 120 current employees and 19 (27 percent) of 71 current external users.

[2] The risk related to the issues discussed in Chapter 3 is rated as High because they present risks or effects that if not addressed could substantially affect the audited entity's ability to effectively administer the program(s)/function(s) audited. Prompt action is essential to address the noted concern(s) and reduce risks to the audited entity.

[3] *An Audit Report on the Department of Family and Protective Services' Adult Protective Services Investigations*, State Auditor's Office Report No. 18-041, August 2018.

The Department did not have an effective process to review user accounts for periods of inactivity. Not disabling access to IMPACT as required by Department policies increases the risk that users could inappropriately access the system.

The Department should strengthen its annual IMPACT user access review process.

The Department implemented a process to annually verify IMPACT users' security profiles to determine whether access levels were still needed and to make any necessary changes.

For the internal and external IMPACT users that auditors tested, the Department's annual user access review was effective in determining that current users' security profiles were appropriate and in identifying when a change to a user's profile was needed. However, the Department's annual user access review did not identify the applicable employees who stopped working with the Department and who no longer needed access to IMPACT.

The Department did not perform renewal background checks for external IMPACT users in accordance with its policies.

The Department obtained initial criminal and background checks for all applicable employees and external users that auditors tested. For employees and external users hired while the Department was a part of the Health and Human Services Commission (Commission), the Department relied on criminal and background checks that the Commission performed.

The Department's policies require its divisions sponsoring external users of IMPACT to submit annual renewal background checks for those users. However, the Department did not ensure that 13 (33 percent) of 39 external users received renewal background checks in accordance with its policies. Not ensuring that background checks have been performed increases the risk that an external user will gain unauthorized access to IMPACT.

Recommendations

The Department should:

- Strengthen its controls to disable user accounts when users are no longer working for the Department.
- Implement a process to ensure that it disables IMPACT user accounts when users have not accessed IMPACT within 30 days.
- Comply with its policies to perform renewal background checks for external IMPACT users on an annual basis.

Management's Response

Recommendations #1 and #2:

The Department should:

- *Strengthen its controls to disable user accounts when users are no longer working for the Department.*
- *Implement a process to ensure that it disables IMPACT user accounts when users have not accessed IMPACT within 30 days.*

Management's Response:

The agency is implementing new processes to ensure network accounts are terminated timely when people leave the agency. IMPACT cannot be accessed with a suspended or disabled network account. Network accounts are suspended after 30 days of inactivity. Daily reports are being run showing terminations, and IMPACT is being disabled from these daily reports. DFPS is now disabling access to IMPACT at 30 days of inactivity and is no longer waiting for confirmation from the third party or contract sponsor.

Responsible Person, Title: *Director, Application and Data Support*

Implementation Date: *November 22, 2021*

Recommendation #3:

The Department should:

- *Comply with its policies to perform renewal background checks for external IMPACT users on an annual basis.*

Management's Response:

The sample of users in which an annual renewal was not completed during this review were HHSC Regulatory staff. DFPS is aware of this deficiency and is working to resolve with HHSC.

HHSC users needing external access to DFPS systems will be required to be in compliance with DFPS background check policies which include an annual and renewal background checks.

Responsible Person, Title: *Program Administrator for DFPS Background Checks and FINDRS*

Implementation Date: *May 2022*

Chapter 4

The Department Did Not Consistently Implement Segregation of Duties in IMPACT

Chapter 4 Rating:

Priority[4]

The Department did not consistently implement controls to ensure that the same individual did not close and approve case stages in IMPACT, or perform consistent monitoring and analysis to determine if it was appropriate for the same individual to close and approve case stages in IMPACT (see text box for more information about case stages). The IMPACT system does not have comprehensive edit controls programmed into the system to prevent persons from closing case stages and submitting the closures to themselves for approval. Specifically, the Department implemented a change in IMPACT that would restrict self-approval for case stages to supervisors; however, this restriction only relates to Adult Protective Services case stages. The Department asserted that it reviews cases if concerns are raised; however, the Department did not perform any additional review to ensure that it was appropriate for the same individual to close and approve case stages in IMPACT.

In addition, auditors identified IMPACT security profiles with increased risk relating to lack of segregation of duties.

The Department should consistently implement segregation of duties in IMPACT for closing and approving case stages.

Based on analysis of IMPACT data for case stage closures that occurred between September 1, 2019, and April 8, 2021, 8 percent (51,431 of 636,714 case stages) of the total case stage closures across all Department program areas were closed and approved by the same individual. Table 3 on the next page shows a breakdown by program area within the Department.

Case Stages in IMPACT

A caseworker enters information for a case stage in IMPACT and closes that stage after completing required activities. The Department's policies require supervisor approval for closing certain stages.

A case in IMPACT can move through multiple stages, from intake through closure. Each stage focuses on specific Department case management activities, client needs, and outcomes. Examples of stages include investigation, child substitute care, adoption, family reunification, and services.

See Appendix 4 for additional information.

Source: Information provided by the Department.

[4] The risk related to the issues discussed in Chapter 4 is rated as Priority because the issues present risks or effects that if not addressed could critically affect the audited entity's ability to effectively administer the program(s)/function(s) audited. Immediate action is essential to address the noted concern(s) and reduce risks to the audited entity.

Table 3

Results of Auditors' Analysis of IMPACT Case Stage Closure Data for Segregation of Duties [a]				
Program Area	Total Case Stages Closed and Approved by the Same Individual	Total Case Stages Closed	Percent of Case Stages Closed and Approved by the Same Individual	Department Policy Allows for Cases to Be Closed and Approved by Same Individual
Adult Protective Services (APS) [b]	4,385	176,976	2%	Yes, for supervisors [c]
Child Protective Services (CPS)	21,336	115,108	19%	Not included in policy
Child Protective Investigations (CPI)	25,206	336,237	7%	Not included in policy
Child Care Investigations (CCI)	504	8,393	6%	No
Totals	**51,431**	**636,714**	**8%**	

[a] The IMPACT data included case stages that were closed from September 1, 2019, through April 8, 2021.

[b] In 2018, the State Auditor's Office conducted an audit and identified 2,056 APS investigations closed from September 1, 2016, through January 31, 2018, in which the supervisor closed and approved the same investigation. In that audit, the Department asserted that high caseloads and caseworker turnover resulted in a business need to allow supervisors to close cases and approve cases for closure. See *An Audit Report on the Department of Family and Protective Services' Adult Protective Services Investigations* (State Auditor's Office Report No. 18-041, August 2018).

[c] The APS policies and procedures allow a supervisor to approve cases on his or her own workload when there is a business need.

Sources: Analysis performed by auditors using data from IMPACT; Department policies and procedures; and information from the Department.

The Department asserted that having the same person close and approve some case stages is appropriate in certain circumstances. Examples include:

- When there is a business need to address case stages due to high staff turnover and/or high caseloads.
- When work does not involve direct case management, such as stages relating to placing children from other states in Texas. (These stages involve tracking communications and collaboration with the other state that is performing the case management services.)
- When a supervisor revises a case stage as part of the approval process. (IMPACT will identify that the supervisor made the most recent edit to a closed case stage and approved the case stage.)

Auditors reviewed a sample of 30 case stages that were closed and approved by the same person and identified that both a caseworker and a supervisor entered information into the stage record; however, IMPACT does not provide enough information in the case history to identify exactly which information fields were edited by each individual who worked in the stage.

The Department asserted that unless the person making a revision describes the change in the case narrative, IMPACT will not identify what change was made. As a result, the Department may not know the extent of the changes that are occurring in the instances where this is happening.

Allowing staff to close and approve their own work increases the risk that inappropriate changes could be made to case information in IMPACT or that investigations could result in client safety not being addressed.

Auditors identified some IMPACT security profiles that have an increased risk relating to lack of segregation of duties.

The Department assigns various security profiles to IMPACT users based on each user's position, job duties, regional location, and program. One user can have multiple security profiles, and combinations of abilities within certain profiles could circumvent segregation-of-duties controls.

Auditors identified certain weaknesses related to combinations of abilities within IMPACT security profiles that could result in a risk of lack of segregation of duties if these profiles were assigned. To minimize security risks, auditors communicated details about these issues directly to the Department's management in writing.

Recommendations

The Department should:

- Implement guidance, policies, or practices for its program areas to either prevent the same person from closing and approving case stages or ensure that it was appropriate for the same person to close and approve case stages.
- Implement a process to identify instances of the same individual closing and approving case stages to determine if the self-approvals were appropriate.
- Ensure that it enforces segregation of duties when determining combinations of abilities within security profiles to assign to IMPACT users.

Management's Response

Recommendations #1 and #2:

The Department should:

- *Implement guidance, policies, or practices for its program areas to either prevent the same person from closing and approving case stages or ensure that it was appropriate for the same person to close and approve case stages.*

- *Implement a process to identify instances of the same individual closing and approving case stages to determine if the self-approvals were appropriate.*

Management's Response APS:

Recommendation 1: The Adult Protective Services handbook includes policy in sections 14100 and 14200 on who may approve stage closure. These policies state a supervisor or designee may approve stage closure on his or her own workload only when there is a business need, as determined by the program administrator or district director. The supervisor or designee must document management's approval to self-approve stage closure in IMPACT.

Changes were made to IMPACT in May 2020 to prevent anyone with the role of caseworker in IMPACT from approving stage closures.

Recommendation 2: APS has access to reports in Data Warehouse which contain statistical information related to performance management. Report svc_aps_02 identifies cases pending supervisor approval, including the approver name.

Additionally, inv_aps_20 & 26 identify who rejected a case. The APS state office Management Analyst will run these reports quarterly and provide them to the Director of Policy and Performance. These reports will be used to complete a review of cases to determine if justification for a supervisor or designee to self- approve stage closure for cases on his or her own workload, was documented and appropriate.

Responsible Person, Title: *APS, Policy Manager*

Implementation Date: *May 2020*

Management's Response CPS:

Recommendation 1: CPS will edit and clarify policies 1433 and 1461 to include no one person assigned primary on any case can approve the case closure. The edits will also clarify that case closures must only be approved by supervisors and above. Implementation start date for policy revisions is November 15, 2021.

Recommendation 2: CPS Program Strategy will complete a quarterly review of cases that were closed by a staff person who was primarily assigned the case. Implementation start date for the quarterly case reviews starts with a DRIT to pull data in 3rd quarter FY22 (March/April/May). Case reviews will start in June 2022.

As a long-term solution, CPS will initiate a request for an IT project to change IMPACT and prevent inappropriate closures from occurring. This IT project would be similar to the APS IMPACT project developed to address this issue. Implementation start date for IT project request is November 15, 2021.

Responsible Person, Title: *CPS, Director of Family Preservation and Program Strategy*

Implementation Date: *June 2022*

Management's Response CPI:

CPI Program determined that current policy states that a supervisor has to approve stage closures; however, CPI will provide additional clarity to the follow policies.

Recommendation 1: Updates will be made to Policy section 2292 (Taking Action on a Submitted Investigation). For further clarification, CPI will add to policy "If a supervisor has worked the case as primary, completed substantial contacts or has taken actions to address child safety, that supervisor must save and submit the case to a program director for closure." Communication to the field will be sent out in regard to the changes made to policy once the updated policy has been published.

Recommendation 2: A Data Request Intake and Tracking (DRIT) will be implemented to address the recommendation of "Implement a process to identify instances of the same individual closing and approving case stages to determine if the self-approvals were appropriate." This will help track trends in case closure and related events.

Responsible Person, Title*: CPI, Deputy Director of Investigations & Alternative Response*

***Implementation Date**: January 31, 2022*

Management's Response CCI:

For Child Care Investigations, there is no policy currently in place setting guidelines when it is appropriate and allowable for the person closing the case to be the same person approving the case for closure. There are, however, times where this is appropriate. CCI will be doing the following:

Recommendation 1: Create and implement policy to allow for the closing person and the approving person to be the same person. This will be for limited situations where a supervisor completes minor, non-investigative tasks such as person or case merges, clerical changes, or minor grammatical corrections. A complete list will be formulated by the CCI director and other staff as needed.

Recommendation 2: Add a task for the CCI Quality Assurance Team to complete when reading cases to check to see if the person closing the case and the person approving the case are the same person. If they are the same person, a CCI Manager III or higher will be notified to review whether or not the closing/approval was appropriate.

***Responsible Person(s), Title:** CCI Director and CCI Deputy Director*

***Implementation Date:** December 15, 2021*

Recommendation #3:

The Department should:

Ensure that it enforces segregation of duties when determining combinations of abilities within security profiles to assign to IMPACT users.

Management's Response:

Program Support will coordinate with the areas that use these profiles to ensure IMPACT appropriately supports their separation of duty controls.

In addition to Program Support's annual IMPACT security audit of user permissions, the team is implementing a QA process to check a percentage of eMACs processed each month to verify they were completed correctly. The Identity and Access Management group will provide Program Support a monthly eMAC report designed to strengthen controls for this process.

***Responsible Person, Title:** Director, Application and Data Support*

***Implementation Date:** November 22, 2021*

Chapter 5

The Department Implemented Controls to Secure and Protect the Data in IMPACT, But It Should Strengthen Its Documentation Processes and Compliance With Policies

The Department appropriately documented business need and justification for changes to IMPACT; ensured that changes were developed and tested before being put into production; and maintained segregation of duties among employees who developed, tested, and implemented system changes. However, it should improve its documentation of IMPACT change approvals.

The Department's agreements with external parties helped ensure that IMPACT data was protected and that appropriate access was granted to external users; however, the Department did not consistently comply with its policies for forming and approving these agreements.

The Department deleted cases from IMPACT in accordance with its procedures, but it did not have supporting documentation to show supervisor approval for 5 (13 percent) of the 38 cases deleted between September 1, 2019, and April 8, 2021.

The Department implemented automated controls to help ensure that data in IMPACT is protected.

Chapter 5-A

The Department Appropriately Documented Business Need and Justification for Changes to IMPACT, But It Should Improve Documentation of IMPACT Change Approvals

Chapter 5-A Rating:

Medium[5]

The Department established a change management process for evaluating, approving, and implementing changes to IMPACT (see text box on the next page for information about change management). For the sample of 76 IMPACT changes made between September 1, 2019, and April 8, 2021, that auditors tested, the Department:

- Appropriately documented the description, business need, and justification for changes in its change management systems.

[5] The risk related to the issues discussed in Chapter 5-A is rated as Medium because the issues present risks or effects that if not addressed could moderately affect the audited entity's ability to effectively administer the program(s)/function(s) audited. Action is needed to address the noted concern(s) and reduce risks to a more desirable level.

- Ensured that changes were developed and tested before being put into production.
- Maintained segregation of duties among employees who developed, tested, and implemented changes to reduce the risk that one person could make inappropriate changes to IMPACT.

Change Management

Change management is the process of managing all changes related to information system infrastructure and applications. Changes can include system enhancements, correcting defects, patches, and emergency changes. The change management process includes reviewing and approving proposed changes, documenting those decisions, and retaining records about those changes. Changes should be reviewed against planned outcomes following the implementation.

Sources: Department of Information Resources' *Security Control Standards Catalog*, Version 1.3, and information provided by the Department.

Change Management Approval. The Department established a Change Approval Board (Board) that meets weekly and as needed to approve development and testing of changes and moving the changes into production. For 7 (9 percent) of the 76 changes auditors tested, the Board's meeting minutes and records did not show approval prior to the changes being moved into production.

The Department's policies require that (1) the Board ensure that only organization-approved changes are deployed; (2) approvals of change requests are obtained from the Board; and (3) decisions regarding change requests are recorded. If the changes are not documented in the Board's meeting minutes, there is no evidence that the Board approved implementation of the change in IMPACT. In addition, not obtaining the Board's review and approval before the change is released into production increases the risk that inappropriate changes could be introduced into IMPACT, which could result in loss of data or system functionality.

Recommendation

The Department should ensure that its Change Approval Board complies with its policies to document the Board's decisions.

Management's Response

As of November 1, 2021, DFPS revised the Change Approval Board's (CAB) process to include documenting the CAB approval and CAB release dates in the Project and Portfolio Management system (PPM). DFPS also revised the Request for Change Form to include Emergency CAB (eCAB) information. Lastly, DFPS created and delivered CAB process refresher training classes to appropriate staff. CAB process documents will be updated to match the revised CAB process.

Responsible Person, Title: *Interim IT Operations Director*

Implementation Date: *December 3, 2021*

Chapter 5-B

The Department's Agreements With External Parties Helped Ensure That IMPACT Data Is Protected; However, the Department Did Not Consistently Comply With Its Policies to Form and Approve the Agreements

Chapter 5-B Rating:

Low[6]

Between September 1, 2019, and April 8, 2021, the Department was a party to 17 agreements that (1) established and managed data exchanges between IMPACT and systems outside of the Department and/or (2) granted IMPACT access to external users. Those agreements helped ensure that IMPACT data was protected and that appropriate access was granted to external users; however, the Department did not consistently comply with its policies for forming and approving these agreements.

The Department's agreements with external parties helped ensure that confidential data was protected.

The Department's policies require agreements to include provisions that obligate the other party to protect confidential information. Auditors identified provisions requiring the protection of confidential information in all 17 agreements tested.

The Department also ensured that all 137 external users with access to IMPACT that auditors tested had signed security agreements, which required the users to certify that they will protect confidential information and comply with Department information security requirements.

The Department did not consistently comply with its policies when forming agreements with external parties.

The Department established policies that required (1) agency officials to document approval using a routing form and (2) specific elements to be included in its agreements with external parties. The Department did not consistently comply with those policies. Specifically:

- The Department did not document the approval for 6 (40 percent) of 15 agreements using the routing form. The Department was not required to use the routing form for the remaining two agreements, because the

[6] The risk related to the issues discussed in Chapter 5-B is rated as Low because the audit identified strengths that support the audited entity's ability to administer the program(s)/function(s) audited or the issues identified do not present significant risks or effects that would negatively affect the audited entity's ability to effectively administer the program(s)/function(s) audited.

policy requiring the form was not effective until after the agreements were signed.

- For 1 (13 percent) of 8 agreements tested, the Department did not include a provision that required the other party to notify the Department within 24 hours if an external user stopped working for the other party. This requirement did not apply to the other nine agreements because those agreements did not establish external users for the other party or because the policy was not in place until after the agreement was signed. Not including this provision increases the risk that external users will have unauthorized access to the data in IMPACT.

Recommendation

The Department should comply with its contract formation policies by using routing forms for approval of all agreements and by including required elements in all agreements.

Management's Response

Contract Oversight and Support and the Office of General Council will review agency policy to determine appropriate modifications to the routing of agreements with external parties and ensure communication on expectations is clear. Training will be delivered to support agency personnel.

Responsible Person, Title: *Director of Contract Oversight and Support*

Implementation Date: *August 31, 2022*

Chapter 5-C

The Department Complied With Its Procedures for Deleting Cases from IMPACT, But It Should Ensure That It Retains Documentation to Support Approval of Deletions

Chapter 5-C Rating:

Low[7]

The Department deleted cases from IMPACT in accordance with its procedures; however, it did not have supporting documentation to show supervisor approval for 5 (13 percent) of the 38 cases deleted between September 1, 2019, and April 8, 2021.

The Department established procedures to delete from IMPACT those cases that cannot be processed and need to be recreated due to technical defects. When Department staff encounter technical issues in IMPACT that prevent them from processing a case, they request case deletions using a form that requires information about the reason for deletion. A supervisor must approve the deletion and route the form to the appropriate division for deletion.

The Department's records retention schedule requires that the documentation related to deleted cases be retained for 10 years.

Recommendation

The Department should ensure that it retains documentation to support the deletion of cases from IMPACT in accordance with its record retention requirements.

Management's Response

SWI will create restricted permission folders on the SWI Share Drive where the documentation related to deleted cases will be stored.

Deleted case documentation are those templates that contain the deletion request, report number, case name, and any other relevant information provided including appropriate supervisor approval.

Responsible Person, Title: *SWI Division Administrator of Operations*

Implementation Date: *December 1, 2021*

[7] The risk related to the issues discussed in Chapter 5-C is rated as Low because the audit identified strengths that support the audited entity's ability to administer the program(s)/function(s) audited or the issues identified do not present significant risks or effects that would negatively affect the audited entity's ability to effectively administer the program(s)/function(s) audited.

Chapter 5-D

Automated Controls Protect Data in IMPACT

Chapter 5-D Rating:

Low[8]

The Department implemented automated controls in IMPACT to help protect data in the system.

Auditors tested automated controls related to accessibility and ability to modify case stage and case status types (see Chapter 4 for information about case stages in IMPACT). The controls ensure that:

- Information contained in closed stages of nonsensitive cases cannot be changed by caseworkers or supervisors. IMPACT users can view the stage information, but cannot change it.
- Caseworkers and supervisors with the appropriate IMPACT security profile can view information contained in closed stages of sensitive cases (see text box) but cannot change the information.
- Only caseworkers and supervisors who are assigned to open stages of sensitive cases and who have the appropriate IMPACT security profile can view and change information in sensitive cases.
- Only caseworkers and supervisors assigned to open stages of nonsensitive cases can change information in those stages. Other IMPACT users not assigned to the stages can view the information but are not able to change it.

Sensitive Cases

Sensitive cases are high-profile cases for which access in IMPACT is restricted. Supervisor approval is usually required for designating a case as sensitive.

Sources: Department Statewide Intake policies and procedures and information provided by the Department.

[8] The risk related to the issues discussed in Chapter 5-D is rated as Low because the audit identified strengths that support the audited entity's ability to administer the program(s)/function(s) audited or the issues identified do not present significant risks or effects that would negatively affect the audited entity's ability to effectively administer the program(s)/function(s) audited.

Appendices

Appendix 1

Objectives, Scope, and Methodology

Objectives

The objectives of this audit were to determine whether the Department of Family and Protective Services (Department) has processes and controls related to the Information Management Protecting Adults and Children in Texas (IMPACT) system to ensure that:

- Access to the system is appropriately managed.
- There are key controls to secure and protect the data in the system and these controls are working as intended.

Scope

The scope of this audit covered the Department's processes and controls related to user access and data security for the IMPACT system from September 1, 2019, through April 8, 2021. The scope also included a review of significant internal control components related to user access and data security (see Appendix 3 for more information about internal control components).

Methodology

The audit methodology included conducting interviews and process walkthroughs with Department management and staff; reviewing applicable statutes and Department policies and procedures; performing user access testing; reviewing cases deleted from IMPACT; testing of changes the Department made to IMPACT; performing analysis of IMPACT case stage closure data; and testing the Department's agreements with external parties related to IMPACT data exchanges and external access to IMPACT. Auditors also performed testing of selected automated controls in IMPACT.

Data Reliability and Completeness

To assess the reliability of the user list extracted from the IMPACT System, auditors (1) observed the Department staff extract the user list from IMPACT, (2) reviewed the query parameters and filters used to extract the list, and (3) compared the list of internal IMPACT users to an employee list provided by the Department's Human Resources staff.

To assess the reliability of the list of changes to IMPACT during the audit scope extracted from the Department's Project Portfolio Management (PPM) system, auditors (1) observed as Department personnel demonstrated how they extracted the data from PPM, (2) reviewed the query parameters and filters used to extract the data from PPM, (3) compared the data from PPM to the corresponding data from the Department's Application Lifecycle Management (ALM) system that is used to document testing and development information, and (4) extracted some of the data directly from PPM and ALM using read-only access provided by the Department.

To assess the reliability of the list of agreements for data exchanges between IMPACT and agencies external to the Department, auditors compared the list of agreements to a list of automated jobs from the scheduling system used at the State data center.

To assess the reliability of the IMPACT case stage closure data sets extracted from IMPACT, auditors (1) reviewed query parameters and filters used to extract the data and (2) compared the data to the related cases in IMPACT for a sample of stages.

To assess the reliability of information maintained in a spreadsheet provided by the Department to track cases deleted from IMPACT, auditors (1) compared the cases marked for deletion in the spreadsheet to the Health and Human Services Commission Remedy system tickets that are used to route and process deletions, (2) reviewed queries used to extract the Remedy ticket data, and (3) performed analysis of information in the spreadsheet for reasonableness.

Auditors determined that the data sets listed above were sufficiently reliable for the purposes of the audit.

Sampling Methodology

IMPACT User List. Auditors selected random and nonrandom samples for testing IMPACT user access. Specifically:

- To test internal user access to IMPACT for current and terminated employees (population of 12,145 users from September 1, 2019, through April 8, 2021), auditors selected a nonstatistical sample of 86 users for testing, primarily through random selection. Auditors selected an additional 131 users for testing based on risk, for a total of 217 internal users tested.
- To test external user access to IMPACT for current and terminated users (population of 1,838 users from September 1, 2019, through April 8, 2021), auditors selected a nonstatistical sample of 48 users for testing,

primarily through random selection. Auditors selected an additional 31 users for testing based on risk, for a total of 79 external users tested.

This sample design was chosen to address specific risk factors identified in the population, such as user security profile capabilities in IMPACT. The test results as reported do not identify whether users were randomly selected or selected using professional judgement; therefore, it would not be appropriate to project the test results to the population.

Changes to IMPACT. To test changes made to IMPACT (population of 468 changes made from September 1, 2019, through April 8, 2021), auditors selected a nonstatistical sample of 61 changes for testing, primarily through random selection. Auditors selected an additional 15 changes for testing based on risk, for a total of 76 changes tested. This sample design was chosen to address specific risk factors identified in the population, such as changes that were comprised of 10 or more projects.

The test results as reported do not identify which changes were randomly selected or selected using professional judgement; therefore, it would not be appropriate to project the test results to the population.

Population Testing. Auditors selected the whole population for testing for the following data sets based on risk:

- User access to the Department's network and the IMPACT database and servers (population of 10 users who have individual and shared account access as of April 8, 2021).
- Cases deleted from IMPACT (population of 38 cases that were escalated for deletion from September 1, 2019, through April 8, 2021).
- The Department's agreements with external parties (population of 17 agreements, which includes 14 agreements that establish IMPACT data exchanges and 3 that provide external access to IMPACT, from September 1, 2019, through April 8, 2021).

Information collected and reviewed included the following:

- The Department's policies and procedures.
- The Department's organizational charts.
- IMPACT user list and IMPACT case stage data.
- Password settings for the Department's network and IMPACT database.

- The Department's agreements with external parties related to IMPACT data exchanges and external access to IMPACT.
- Supporting documentation for IMPACT user access, cases deleted from IMPACT, and changes made in IMPACT.
- Minutes from the Department's Information Technology Governance Committee, Architecture Review Board, and Change Approval Board meetings.
- The Department's annual IMPACT user access reviews for fiscal years 2019 and 2020.
- The Department's Disaster Recovery Plan and documentation relating to its testing of the Disaster Recovery Plan.
- System and Organization Controls (SOC) Report related to the State data center vendor's controls for services it provides to the Department.

Procedures and tests conducted included the following:

- Interviews and process walkthroughs with Department management and staff.
- Tested internal and external user access to IMPACT and user access to the Department's network and the IMPACT database and servers.
- Analyzed IMPACT data to identify the number of times the same person closed and approved a case stage.
- Analyzed IMPACT security profiles and user access list to identify security profiles that indicate lack of segregation of duties.
- Tested the Department's automated controls over the IMPACT System.
- Reviewed the SOC Report to gain reasonable assurance about the controls at the State data center vendor that provides services to the Department.
- Tested changes to IMPACT to determine whether changes were adequately documented, properly approved and tested, and moved into production by authorized personnel.
- Tested the password settings for the Department's network and IMPACT database.

- Tested cases deleted from IMPACT for proper review and approval prior to being deleted.
- Tested the Department's agreements with external parties related to IMPACT data exchanges and external access to IMPACT.

Criteria used included the following:

- Title 1, Texas Administrative Code, Chapter 202.
- Texas Government Code, Chapters 2054 and 2059.
- The Department of Information Resources' *Security Control Standards Catalog*, Version 1.3.
- The Department's policies and procedures.

Project Information

Audit fieldwork was conducted from December 2020 through September 2021. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Those standards also require independence in both fact and appearance. During the audit, legislative funding was vetoed. This condition could be seen as potentially affecting our independence in reporting results related to this agency. However, we proceeded with this audit as set forth by the annual state audit plan, operated under the Legislative Audit Committee. We believe this condition did not affect our audit conclusions.

The following members of the State Auditor's staff performed the audit:

- Jennifer Lehman, MBA, CIA, CFE, CGAP (Project Manager)
- Evan Cresap, CPA (Assistant Project Manager)
- Jennifer Brantley, MS, CPA
- Lindsay Escalante, MPSA
- Rebecca Franklin, CISA, CFE, CGAP
- Austin McCarthy, CPA
- Jessica McGuire, MSA

- Erin Hubener Peloquin, CPA, CIDA, CRFAC
- Dana Musgrave, MBA, CFE (Quality Control Reviewer)
- Michael A. Simon, MBA, CGAP (Audit Manager)

Appendix 2

Issue Rating Classifications and Descriptions

Auditors used professional judgment and rated the audit findings identified in this report. Those issue ratings are summarized in the report chapters/sub-chapters. The issue ratings were determined based on the degree of risk or effect of the findings in relation to the audit objective(s).

In determining the ratings of audit findings, auditors considered factors such as financial impact; potential failure to meet program/function objectives; noncompliance with state statute(s), rules, regulations, and other requirements or criteria; and the inadequacy of the design and/or operating effectiveness of internal controls. In addition, evidence of potential fraud, waste, or abuse; significant control environment issues; and little to no corrective action for issues previously identified could increase the ratings for audit findings. Auditors also identified and considered other factors when appropriate.

Table 4 provides a description of the issue ratings presented in this report.

Table 4

Summary of Issue Ratings	
Issue Rating	**Description of Rating**
Low	The audit identified strengths that support the audited entity's ability to administer the program(s)/function(s) audited or the issues identified do not present significant risks or effects that would negatively affect the audited entity's ability to effectively administer the program(s)/function(s) audited.
Medium	Issues identified present risks or effects that if not addressed could moderately affect the audited entity's ability to effectively administer the program(s)/function(s) audited. Action is needed to address the noted concern(s) and reduce risks to a more desirable level.
High	Issues identified present risks or effects that if not addressed could substantially affect the audited entity's ability to effectively administer the program(s)/function(s) audited. Prompt action is essential to address the noted concern(s) and reduce risks to the audited entity.
Priority	Issues identified present risks or effects that if not addressed could critically affect the audited entity's ability to effectively administer the program(s)/function(s) audited. Immediate action is required to address the noted concern(s) and reduce risks to the audited entity.

Appendix 3

Internal Control Components

Internal control is a process used by management to help an entity achieve its objectives. The U.S. Government Accountability Office's *Government Auditing Standards* require auditors to assess internal control when internal control is significant to the audit objectives. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) established a framework for 5 integrated components and 17 principles of internal control, which are listed in Table 5.

Table 5

Internal Control Components and Principles		
Component	**Component Description**	**Principles**
Control Environment	The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure.	▪ The organization demonstrates a commitment to integrity and ethical values. ▪ The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control. ▪ Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives. ▪ The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives. ▪ The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.
Risk Assessment	Risk assessment is the entity's identification and analysis of risks relevant to achievement of its objectives, forming a basis for determining how the risks should be managed.	▪ The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives. ▪ The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed. ▪ The organization considers the potential for fraud in assessing risks to the achievement of objectives. ▪ The organization identifies and assesses changes that could significantly impact the system of internal control.
Control Activities	Control activities are the policies and procedures that help ensure that management's directives are carried out.	▪ The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels. ▪ The organization selects and develops general control activities over technology to support the achievement of objectives. ▪ The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.

Internal Control Components and Principles		
Component	**Component Description**	**Principles**
Information and Communication	Information and communication are the identification, capture, and exchange of information in a form and time frame that enable people to carry out their responsibilities.	▪ The organization obtains or generates and uses relevant, quality information to support the functioning of internal control. ▪ The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control. ▪ The organization communicates with external parties regarding matters affecting the functioning of internal control.
Monitoring Activities	Monitoring is a process that assesses the quality of internal control performance over time.	▪ The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning. ▪ The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

Source: Internal Control – Integrated Framework, Committee of Sponsoring Organizations of the Treadway Commission, May 2013.

Appendix 4

Case Stages in IMPACT

Table 6 provides information on some of the case stages that the Department of Family and Protective Services (Department) uses in IMPACT, including the activities that are involved, which program the stages apply to, and whether supervisor approval is required to close the stage.

Table 6

Case Stage Descriptions, Programs That Use the Stages, and Whether Supervisor Approval Is Needed to Close the Stage			
Stage Abbreviation	**Stage Description (in alphabetical order)**	**Program [a]**	**Supervisor Approval Required to Close**
A-R	Alternative Response. It is an alternate way for investigators to respond to certain types of allegations. A-R cases do not have a final case disposition of abuse or neglect or a designation of a perpetrator.	CPI	Yes
ADO	Adoption. Stage is opened before a child enters an adoptive placement. The ADO stage is closed once the adoption is consummated.	CPS	Yes
AOC	Aging out of Care. This stage is for a child in Department conservatorship who may need guardianship services past age 17.	APS	Yes
FAD	Foster and Adoptive Home Development. When the Department receives an inquiry from a family about becoming verified or approved to foster or adopt children in Department conservatorship.	CPS	Yes
FPR	Family Preservations (also known as family based safety services). Helps families who need additional services to keep a child safe and prevent entry into substitute care.	CPS	Yes
FRE	Family Reunification. For a parent or parents who are receiving family reunification services when all children previously in substitute care are returned to the home of the parent or parents, but the Department maintains conservatorship.	CPS	Yes
FSU	Family Substitute Care. Established for a family that is receiving services from the Department because one or more children were removed from the home and are placed outside the home in substitute care.	CPS	Yes
INT	Intake. The first stage in every case. A report that involves allegations of abuse, neglect, or exploitation. Intake specialists use relevant state statutes, program policy, and program guidelines to determine the appropriate program, allegations, and priority for each intake.	APS, CCI, CPI, and CPS	No
INV	Investigation. The stage begins with the decision to investigate a report and includes a disposition for each allegation, assessment of risk and safety, and determination of whether protective services should be provided.	APS, CCI, CPI, and CPS	Yes
KIN	Kinship. Established when a kinship caregiver is caring for a child in Department conservatorship.	CPS	Yes
PAD	Post-Adoption. After an adoption is consummated. If the family requests post-adoption services later, the closed case is reopened.	CPS	No

Case Stage Descriptions, Programs That Use the Stages, and Whether Supervisor Approval Is Needed to Close the Stage			
Stage Abbreviation	Stage Description (in alphabetical order)	Program [a]	Supervisor Approval Required to Close
PAL	Preparation for Adult Living. Youth who are in a Child Substitute Care (SUB) stage at age 14. The PAL stage ends when the youth or young adult is no longer receiving services.	CPS	No
PCA	Permanency Care Assistance. Provides financial support to relative or fictive kin caregivers who take permanent legal responsibility for a child.	CPS	No
SUB	Child Substitute Care. Established for a child who is in the temporary or permanent managing conservatorship of the Department.	CPS	Yes
SVC	Services. Includes maintenance services and intensive care services.	APS	Yes

[a] Programs include the following:

- Adult Protective Services (APS).
- Child Care Investigations (CCI).
- Child Protective Investigations (CPI).
- Child Protective Services (CPS).

Sources: The Department's policy handbooks and information provided by the Department.

Copies of this report have been distributed to the following:

Legislative Audit Committee

The Honorable Dan Patrick, Lieutenant Governor, Joint Chair
The Honorable Dade Phelan, Speaker of the House, Joint Chair
The Honorable Jane Nelson, Senate Finance Committee
The Honorable Robert Nichols, Member, Texas Senate
The Honorable Greg Bonnen, House Appropriations Committee
The Honorable Morgan Meyer, House Ways and Means Committee

Office of the Governor

The Honorable Greg Abbott, Governor

Department of Family and Protective Services

Ms. Jaime Masters, Commissioner