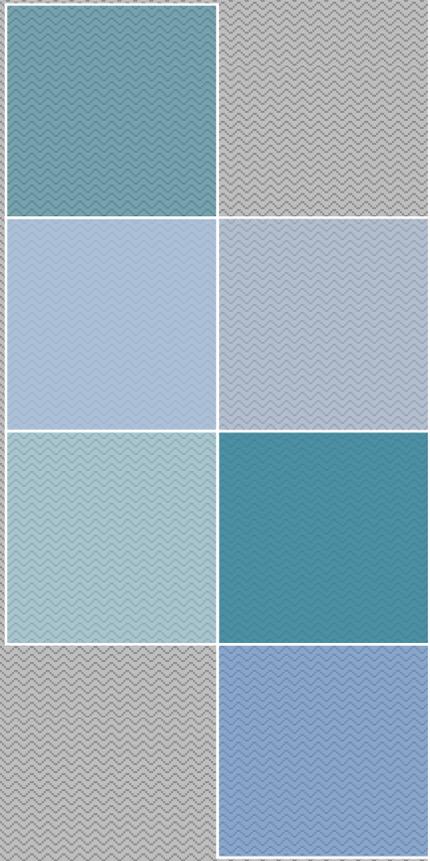


2019

Travis County Auditor's Office Risk Assessment for Travis County Constable, Precinct 4

#18-13



TRAVIS COUNTY
AUDITOR'S OFFICE

PATTI SMITH, CPA
COUNTY AUDITOR



TRAVIS COUNTY
700 LAVACA
P.O. BOX 1748
AUSTIN, TX 78767
(512) 854-9125
FAX: (512) 854-9164

To: Constable George Morales
Constable, Precinct 4

From: Patti Smith, CPA
Travis County Auditor

Date: May 3, 2019

Re: 2018 Risk Assessment – Constable, Precinct 4

The Risk Evaluation and Consulting Division (REC) of the Travis County Auditor's Office has completed a risk assessment of the Constable, Precinct 4 (CN4) Office. The objective of the risk assessment was to assist CN4 in identifying potential risks or exposures associated with their business processes, allowing them to implement or adjust internal controls as they deemed necessary.

We began by performing an engagement-level inherent risk assessment focusing on identifying and rating risks that are intrinsic to CN4's activities and business processes. To a limited extent, we considered the impact of internal controls implemented by management to mitigate these risks. As such, the reported risks represent potential exposures. While we are not providing a judgment of how well management is addressing risk, we have noted some "areas of concern" that involve a variety of issues, risks, and potential control items.

A summary of our methods and results comprises the first eight pages of this report. The organizational structure and financial data for CN4 are provided on pages 13 through 15. The details of the office's risk assessment, including the missions and objectives, significant activities, identified business processes, inherent risks and ratings, and areas of concern, can be found starting on page 16.

BACKGROUND

Constables' Offices serve as law enforcement agencies for Travis County, with county-wide jurisdiction in civil and criminal matters. They process and execute civil legal notices, summonses, and citations from various courts, including forcible entry and detainers, writs of possession, citations, and executions issued from the justice of the peace courts.

The constables also process and execute misdemeanor traffic and hot check warrants of arrest for the Travis County Justices of the Peace courts, as well as other municipalities and counties.

SCOPE

The risk assessment covered the operations of CN4 and was limited to the business processes that were in place during the time the risk assessment was being performed - the three months ending September 30, 2018. In addition, only the inherent risks were rated, meaning there were no tests of controls or transactions to assess control risk. All client meetings were held at the CN4 Office.

ENGAGEMENT TEAM

Amanda Muehlberg, CPA, Lead Auditor
Tracey Powers, Staff Auditor

CLOSING

This report is intended solely for the information and use of the CN4 Office, the Auditor's Office, and County management. We greatly appreciate the cooperation and assistance received from management and staff during this risk assessment. Please contact our office if you have any concerns or questions regarding this report.



David Jungerman, CIA
Chief Assistant County Auditor II – Risk
Evaluation & Consulting



Patti Smith, CPA
Travis County Auditor

REPORT DISTRIBUTION

Lora Livingston, Judge, 261st Judicial District
Brenda Kennedy, Judge, 403rd Judicial District
Sarah Eckhardt, Travis County Judge
Jeff Travillion, Commissioner, Precinct 1
Brigid Shea, Commissioner, Precinct 2
Gerald Daugherty, Commissioner, Precinct 3
Margaret Gomez, Commissioner, Precinct 4
Jessica Rio, County Executive, Planning and Budget Office
Bryon Curtis, Office Manager Senior, Constable, Pct. 4
Joe Alvarado, Financial Manager, Constable, Pct. 4
Managers, Travis County Auditor's Office
Travis County Executive Managers
Examination File

INTRODUCTION TO THE RISK ASSESSMENT REPORT FORMAT

WHAT IS RISK ASSESSMENT?

Risk assessment is a systematic process of evaluating the potential negative outcomes, such as financial loss, that may occur in a business process.

HOW DOES THE RISK ASSESSMENT PROCESS WORK?

The risk assessment process includes three steps: data gathering; business process, risk and control identification; and risk rating. In data gathering, we collect information about the functional area under review to gain an understanding of its objectives, operations, and processes. We then identify what processes are in place, the inherent risks for each process, and the internal controls that have been implemented by management. The last step is rating the risks identified for the business processes handled by the functional areas under review by evaluating them based on risk factors and assigning risk ratings.

HOW ARE THE RISK RATINGS ON THE RISK PROFILES CALCULATED?

The risks associated with each business process can be described and valued based on the risk factors of impact and likelihood. Impact evaluates the magnitude or effect resulting from a breakdown in the process and/or controls, whereas likelihood is used to evaluate the probability that the event will occur. The components of likelihood include geographic dispersion, complexity of operations, training and documentation, access to high-risk assets, state of automation, abuse of power potential, and management oversight. The components of impact include volume/dollar value/operational significance, media attention, government regulation, and damage to customers or third parties.

In order to obtain a risk rating for these business processes, we assign a numeric value to each of the above components. Likelihood is graded on a 1 to 5 scale from very remote to probable, while impact is graded on a 1 to 5 scale from very light to very severe. The values are then plotted on the Inherent Risk Matrix to determine the risk rating for the individual business process.

HOW IS THIS REPORT USED BY THE AUDITOR'S OFFICE?

We use risk assessments to allocate audit resources, thus prioritizing areas of greatest risk.

HOW CAN THIS REPORT BE USED BY COUNTY MANAGEMENT?

This report is intended to help management focus their efforts on mitigating the highest risk areas. This includes the distribution of personnel, implementation of internal controls, and allocation of budget resources.

EXECUTIVE SUMMARY

PURPOSE

During fiscal year 2013, REC began the process of transitioning to the risk-based method of internal auditing. Under this approach, audit resources are directed toward the higher risk areas first. To determine which County offices/functional areas/business processes pose the greatest risk to the County, risk assessments are performed. The two levels of risk assessment are described below:

ENTERPRISE RISK ASSESSMENT (ERA)

This type of risk assessment is performed annually and involves identifying, rating, and ranking risks at the enterprise or County level. The ERA is performed at a higher level both in terms of risk rating thresholds and level of detail. The results of this assessment are used to create the audit plan which is the schedule of internal audit engagements to be performed during the upcoming year. The audit plan is used to prioritize the utilization of audit resources.

AUDIT/ENGAGEMENT RISK ASSESSMENT (ARA)

Risk assessments performed at the engagement level delve into greater detail than ERAs, as they address the risks associated with the processes and activities handled by the County office or functional area under review. This type of risk assessment requires the internal auditor to gain an understanding of the entity's business objectives, flow of operations, business processes, inherent risks, and the system of internal controls implemented by management. During an ARA, there are three types of risks identified, evaluated, and rated as follows:

- **Inherent risk** – The risk to an organization in the absence of any actions management might take to alter either the risk's probability or impact. In other words, the risks intrinsic to the entity's objectives if no internal controls are implemented.
- **Control risk** – The risk that management controls are not efficiently designed or effectively implemented, preventing the organization from meeting its objectives and protecting its assets.
- **Residual risk** – The risk that remains after management has responded to the risk by implementing controls.

To properly implement risk-based auditing, REC will be performing engagement-level risk assessments of all the Travis County offices and departments. For the majority of these entities, we will only be rating the inherent risks during the initial risk assessment. The audit plan will then be tailored to address the higher risk areas first. Going forward, we will periodically update the ARAs and accordingly adjust the audit plan. This is the first risk assessment for Constable, Precinct 4.

METHODOLOGY

The risk assessment process was performed in three phases: data gathering; business process, risk and control identification; and risk rating. Brief overviews of the phases are provided below:

- **Data Gathering** - Collect sufficient information about the functional area under review to gain an understanding of its business objectives and flow of operations.
- **Identification of business processes, risks and controls** - Determine what business processes are in place, the inherent risks associated with the processes, and the internal controls implemented by management to mitigate the risks.
- **Rate inherent risks** - Evaluate the inherent risks and assign risk ratings to the business processes handled by the functional areas under review.

More information about the ARA process is provided in the detailed report section below.

HIGH RISK AREAS

We rated the risks inherent to the business processes handled by CN4 on a five-level scale from very low to very high. A summary of the risk ratings is presented in graph form on page 8 of this report. The top business processes in terms of inherent risk are provided below.

BUSINESS PROCESSES

To provide visibility into the business processes which pose the greatest risk to CN4, we calculated the average risk rating for each business process. A summary of the average risk ratings for the business processes is presented in graph form on page 12 of this report. The top four business processes in terms of inherent risk are provided below:

<u>Business Process</u>	<u>Risk Rating</u>
Cash Handling	Medium
Facilities	Medium
Fleet	Medium
Fixed Assets	Medium

The inherent risks, risk management techniques, and risk ratings for the business processes are provided in detail within the Business Process Risk Profile which begins on page 16 of this report.

DETAILED REPORT

RISK ASSESSMENT PROCESS

We performed an engagement-level risk assessment of the inherent risks associated with the Travis County Constable, Precinct 4 operations in the following three phases:

DATA GATHERING

In order to perform an accurate and thorough risk assessment, the first step is becoming familiar with the nature of the entity's business activities. To begin this process, we requested the following documents from CN4:

1. Organizational charts
2. Budget submission forms (PB-3s) which provide program goals, statutorily required/mandated services, discretionary services, funding sources, anticipated reductions in revenues and grant resources, performance measures, historical trends, program efficiencies/outcomes, and proposed reallocations of budget
3. Grant listings
4. Contract listings (interlocal, professional services, and revenue)
5. Listing of programs
6. Fee schedules
7. Policies and procedures
8. Formally documented narratives and flowcharts

Before meeting with CN4 employees, we reviewed the above documentation; department website; prior audit reports; Texas statutes pertaining to the responsibilities of CN4; guidance provided by regulatory agencies such as the Office of Court Administration (OCA); various narratives; Commissioners Court Agendas, Backup Support, and Minutes; Travis County Code; and the Comprehensive Annual Financial Report (CAFR).

At the entrance conference, we met with the Senior Court Clerk II at their office located on McKinney Falls Parkway. At this meeting we provided an explanation of how our office performs risk assessments, as well as the anticipated timeline. In addition, we received a high-level overview of their operations.

We subsequently held meetings with office employees and others to discuss their operations and business processes in greater detail. During these meetings, the employees described the various tasks they are required to perform. These responsibilities are captured on their respective risk profiles, which can be found beginning on page 16 of this report. After the meetings, we documented their flow of operations and business processes, following up with staff as needed.

IDENTIFICATION OF BUSINESS PROCESSES, RISKS, AND CONTROLS

After completing the process flow documentation, we analyzed the information gathered for each functional area and identified the following: the auditable business processes, potential risks inherent to these processes, and the controls implemented by management to mitigate the risks. We documented the results of this analysis on the Functional Area Risk Profile provided later in this report. Additional details about the information reported on the risk profile schedule are provided below.

BUSINESS PROCESSES

A business process can be defined as a group of interrelated activities or tasks that are initiated to accomplish a specific organizational goal. In the context of a risk assessment performed by REC, business processes include the basic activities used to support financial operations such as cash handling, accounts payable, contract management, etc. Business processes in place at CN4 include the following:

- Accounts Payable
- Accounts Receivable
- Cash Handling
- Facilities
- Fixed Assets
- Fleet
- General Ledger
- Inventory
- Reporting
- Revenue Generation

POTENTIAL RISKS

To identify the potential risks that could prevent CN4 from achieving their financial objectives, we reviewed the individual steps of their business processes with a focus on what could go wrong that would result in either the failure to meet objectives or in a loss of County funds. We consulted auditing standards for internal and governmental auditors, as well as industry-accepted technical guidance for risk assessment, as needed.

Inherent risks are those risks that exist in the absence of any actions management might take to alter either the risk's probability or impact. Because management control is not a factor in determining the level of inherent risk, a high degree of inherent risk does not indicate poor management or the absence of controls.

REPORTED RISK MANAGEMENT TECHNIQUES/CONTROLS

Risk management techniques/controls were self-reported by division management during the course of interviews and follow-up communications. Although we reviewed their controls for reasonableness, we have not audited or otherwise validated them through audit procedures. After risk management techniques were identified, they were mapped to the risks they were designed to mitigate.

The CN4's staff and management are very dedicated to improving all aspects of their processes, providing excellent customer service, and maintaining the superior reputation of the office.

RATE INHERENT RISKS

PROCESS RISK RATING

We evaluated the business processes and the associated risks for each functional area, rating the risks based on the risk factors of impact and likelihood. Impact evaluates the magnitude or effect resulting from a breakdown in the process and/or controls, whereas likelihood is used to evaluate the probability that the event will occur. We used the following risk factors to evaluate impact and likelihood:

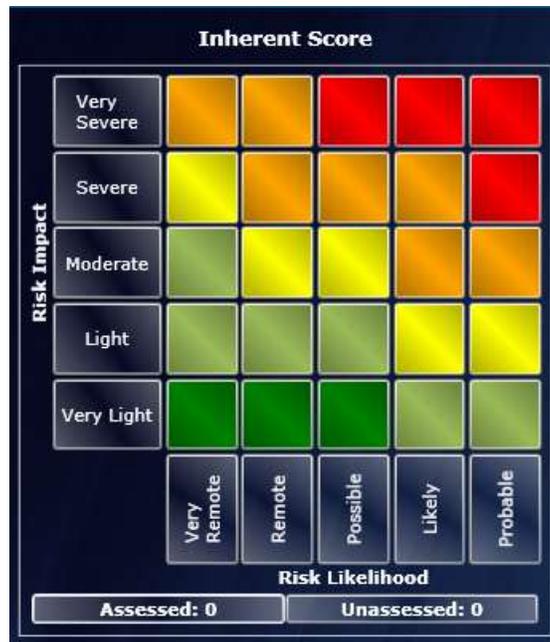
IMPACT

- Volume/dollar value/operational significance
- Media attention
- Government regulation
- Damage to customers or third parties
- Data privacy and protection

LIKELIHOOD

- Geographic dispersion
- Complexity of operations
- Training and documentation
- Access to high-risk assets
- State of automation
- Abuse of power potential
- Management oversight

We rated impact risk on a five-level scale from very light to very severe and likelihood risk from very remote to probable. The resulting scores were then used to determine the overall inherent risk ratings for each business process using our risk matrix, an example of which is provided below:



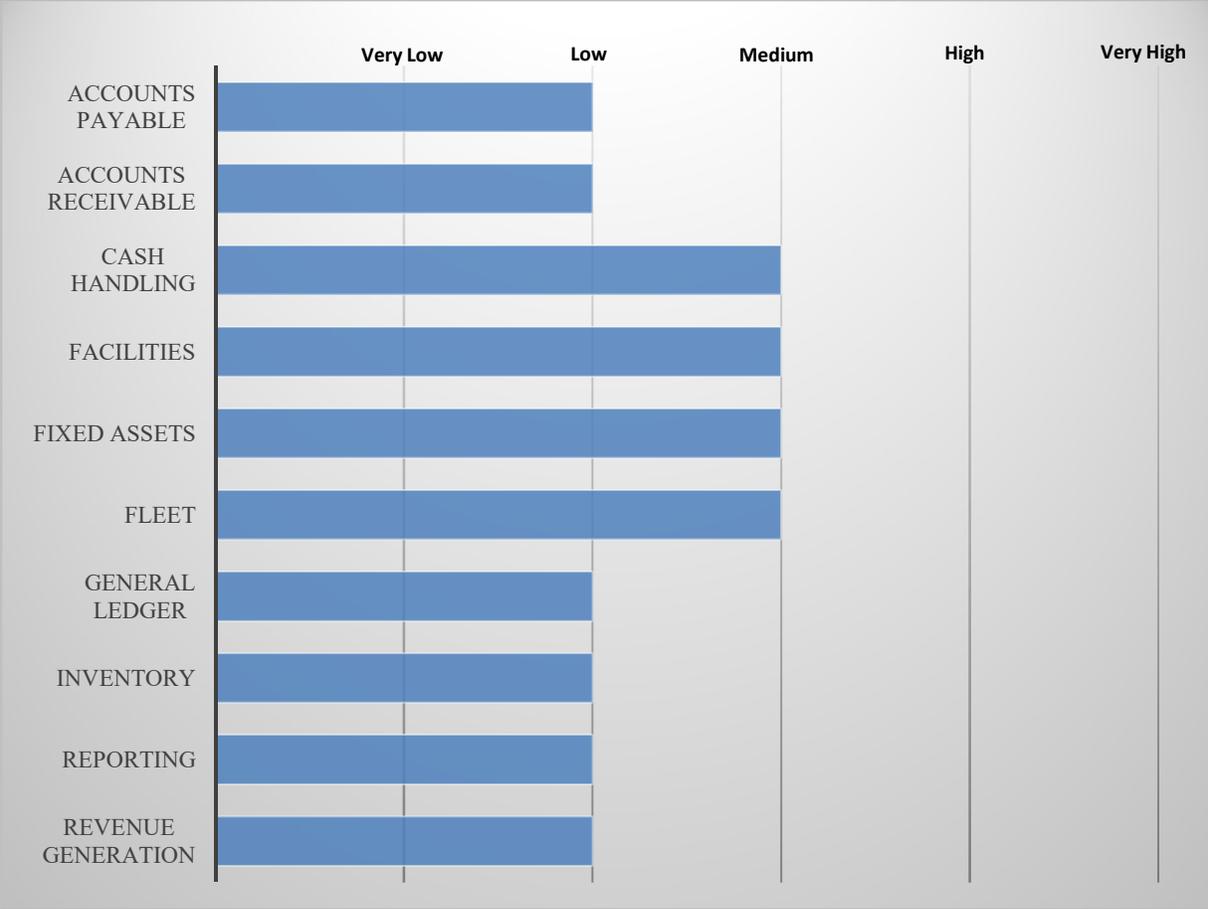
Using this matrix, the inherent risk for each business process was rated on a five-level scale as follows:

Color	Risk Rating	Description
Dark Green	Very Low	The risk of loss is remote or, if a loss were to occur, it would have no material impact.
Light Green	Low	The risk of loss is small and, even if a loss were to occur, it would have little material negative impact.
Yellow	Medium	There is an average risk of loss and, if a loss were to occur, it would likely have a moderate impact on the County.
Orange	High	The activity could potentially result in a significant loss to the County; however, the resulting loss, while significant, would not threaten the County in the long term.
Red	Very High	The activity could lead to significant and harmful loss to the County.

SUMMARY OF RESULTS

GRAPH 1 – RISK PROFILE BY BUSINESS PROCESS

To provide visibility into the business processes which pose the greatest risk to CN4, we present the results in graph form below:



CONSTABLE, PRECINCT 4 ORGANIZATIONAL CHARTS

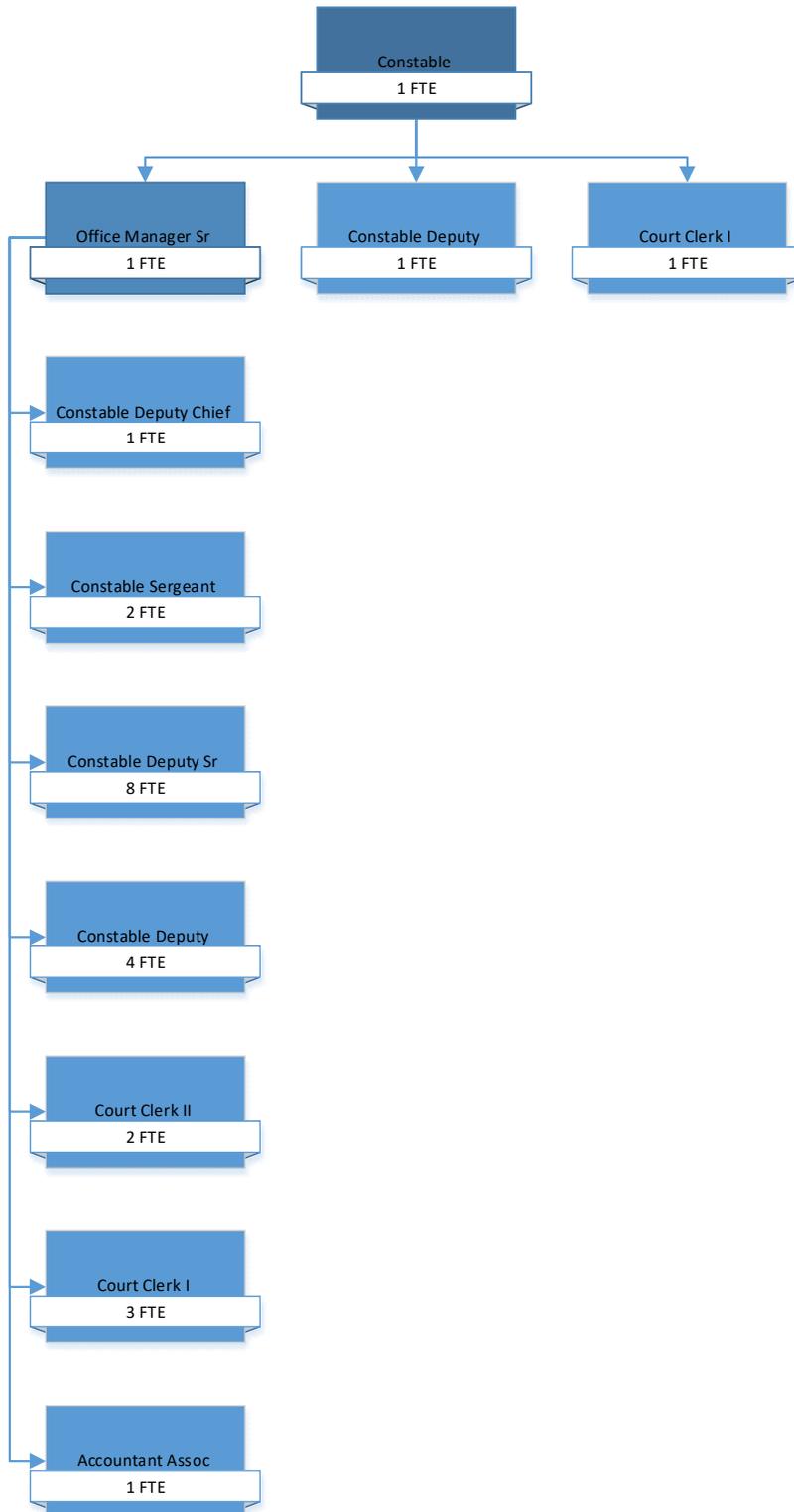


Chart information obtained from SAP – October 2018

Accounting functions for the Constable, Precinct 4 Office are under the Justice of the Peace, Precinct 2 Office for budgeting purposes. For this reason, they are not shown in the organizational chart on the previous page. Below is the organizational chart for the CN4 accounting function.

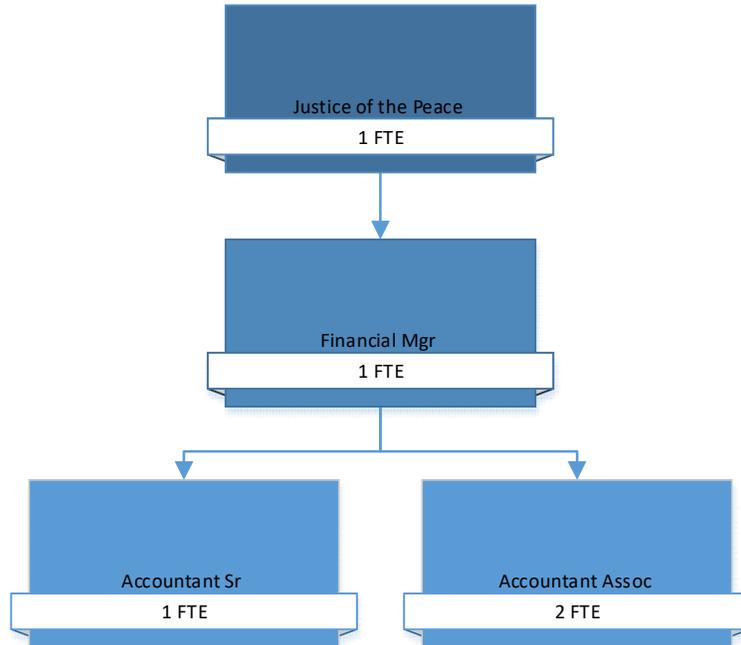
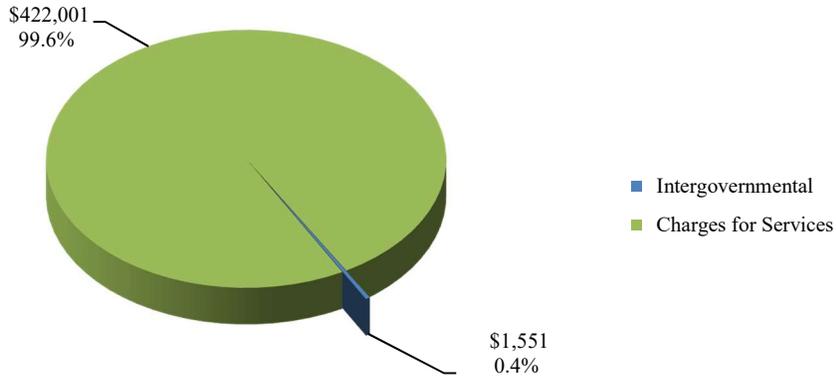


Chart information obtained from SAP – October 2018

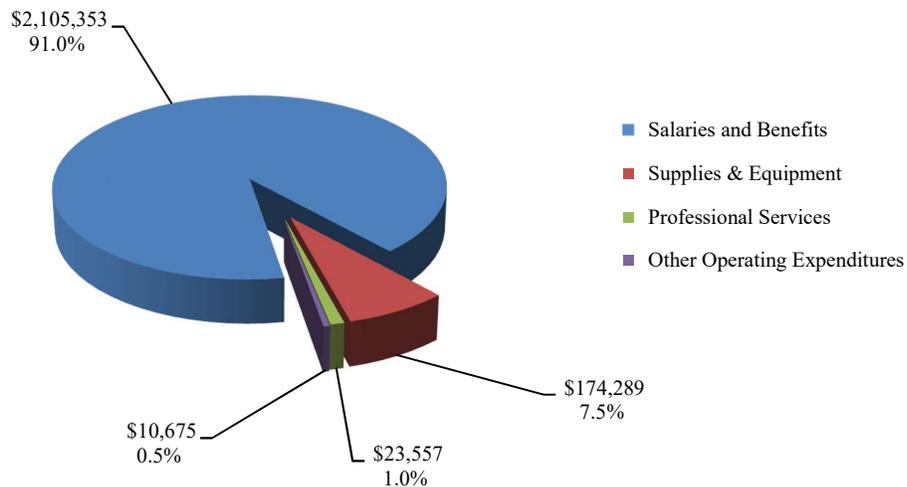
FISCAL YEAR 2018 FINANCIAL DATA

During fiscal year 2018, the Travis County Constable, Precinct 4 received \$1,551 in intergovernmental revenue and \$422,001 in charges for services. Salaries and Benefits, totaling \$2,105,353, represented approximately 91% of their expenditures. The details for their revenue and expenditures are provided below in graphic form:

Revenues



Expenditures



BUSINESS PROCESS RISK PROFILES

MISSION AND OBJECTIVES

The financial component of the Constable, Precinct 4 Office is responsible for receiving and processing the deposit of court costs, fines and fees received both at the office and from field units. This component also processes vehicle donations received.

This component is also responsible for processing disbursements relating to warrants, overpayments, and unclaimed property, as well as posting collections on executions. They also remit funds collected to the appropriate agencies (e.g., the County Treasurer, State of Texas, etc.). In addition, this division prepares monthly departmental financial statements and bank reconciliations.

The operational component of this office is responsible for managing/monitoring fixed assets, supplies, facility work orders, fleet usage, and vehicle maintenance. In addition, all warrants and citations are executed by the operational component of the office.

SIGNIFICANT ACTIVITIES

Accounts Payable

Disbursements processed by a lead financial staff member include: refunds for overpayments, fines and fees due to the Justice of the Peace, Precinct 4 Office and other governmental agencies, writs of execution, and unclaimed funds remitted to the State and/or Treasurer.

Fees due to the Treasurer and Justice of the Peace, Precinct 4 office are remitted via electronic payment on a daily basis and financial staff initiate the entry of these deposits into the SAP financial system. Fees due to other governmental agencies are remitted via check on a daily basis. Refunds for overpayments of \$5 or higher are disbursed weekly. Finally, unclaimed funds that are eligible to be escheated are remitted annually to the State Comptroller and County Treasurer.

Accounts Receivable

Receivables relate primarily to off-duty vehicle donations. Off-Duty vehicle donations are entered into the CivilServe system by clerks using paperwork received from the Sergeant or checks received by mail. Invoices are scanned and attached to the case in CivilServe. In order to review receivables, office personnel create and review an aging report on a quarterly basis.

Given the nature of the work performed by this office, it is rare to have outstanding accounts receivable that requires collection efforts. Office personnel typically receive payments for vehicle donations at the time of service and there are no interlocal contracts currently in place (for either out-of-county warrant work or regular HOA services).

Cash Handling

A lead financial staff member is responsible for reconciling the deposit of collections and completing deposits on a daily basis. The financial staff is also responsible for voiding receipts when necessary, though this is not a regular occurrence.

General Ledger

On a monthly basis, a lead financial staff member reconciles the general ledger accounts to the supporting records, posting journal entries as needed.

Bank Reconciliations

The bank accounts are reconciled on a weekly basis to verify that all funds collected and disbursed per the office accounting records were actually received and paid by the bank (and vice versa). This process also facilitates the correction of any discrepancies. A lead financial staff member performs month-end bank reconciliations in order to verify that the weekly reconciliations are accurate and any discrepancies have been timely corrected. These monthly reconciliations are also used in the preparation of the monthly financial statements.

Reporting

A lead financial staff member reviews system-generated reports, which support the financial statements, to identify errors requiring correction and trends that should be highlighted. When complete, the financial statements are approved and provided to the County Auditor's Office.

General Operations

General Operations is comprised of four separate process areas: facilities, fixed assets, fleet, and inventory. A Sergeant oversees the fleet function and is responsible for overseeing all work orders, maintenance, and disposals/transfers of vehicles. This Sergeant creates a vehicle specifications sheet when new vehicles are approved in the budget and ensures upfit (installation of additional specialized equipment) is completed with the correct equipment. While vehicle maintenance is the responsibility of the deputy assigned to the vehicle, the Sergeant reviews and monitors overall compliance with maintenance schedules, as well as vehicle transfers and disposals.

The Office Manager is responsible for overseeing facilities, fixed assets, and inventory functions, which include managing work orders; ordering, tagging, and tracking fixed assets; and ordering and monitoring inventory (primarily office supplies).

Building security and employee safety also fall under the purview of the facilities function; however, responsibility for this area lies with senior level staff (not just the Office Manager) and the County's Facilities Management Department (FMD) Security Division. The Constable, Precinct 4 Office has an emergency response plan in place that was adapted from the currently accepted and working version for the Precinct 2 Building. It has been submitted to the County Security Manager for review and additional input. The FMD Security Division is in the process of implementing a County Emergency Response and Preparedness Plan, and they will be working with County offices to create site-specific Emergency Action Plans. In addition, a County Security Training employee will be visiting each office location to evaluate office plans and preparedness and train office staff.

BUSINESS PROCESS RISKS AND RISK RATINGS

The following chart depicts the risk ratings for the Constable, Precinct 4 business areas:

Business Process	Risk Rating
Accounts Payable	Low
Accounts Receivable	Low
Cash Handling	Medium
Facilities	Medium
Fixed Assets	Medium
Fleet	Medium
General Ledger	Low
Interlocal Agreements	Low
Inventory	Low
Reporting	Low
Revenue Generation	Low

The following are the primary risk areas/control objectives for this office:

1. Collections (e.g. cash, credit cards, etc.) are properly tracked, reviewed, and accounted for in order to prevent loss or misappropriation.
2. Sufficient cash handling and bank reconciliation controls are in place to help safeguard funds from loss or misappropriation.
3. An Emergency Action and Recovery Plan is in place to address security breaches, employee safety, and catastrophic events.
4. Fixed Assets are tagged and tracked to prevent loss or misappropriation.
5. Vehicles are monitored to ensure that appropriate equipment is installed and maintenance is performed at regular intervals to prevent vehicle downtime.

AREAS OF CONCERN

During our risk assessment, we noted the following controls that do not appear to be sufficiently mitigated by active internal controls:

Cash Handling

Office policy requires that employees preparing daily deposits do not collect and receipt funds; however, these parties do have access to create system-generated receipts. We recommend that office management periodically verify that parties performing daily deposits have not inappropriately created, adjusted, or voided receipts for collections.

Management Response:

We now audit this every day, and any edits are flagged and followed up on. We also limited edit function to two people to reduce the possibility of theft.

General Operations

1. The office does not regularly track odometer readings or service dates for the vehicles assigned to its fleet. Without proper tracking, unnecessary wear and tear could occur, potentially shortening vehicle lifespans and elevating fleet costs.
2. All deputies are issued fuel cards for their vehicles. The TNR Fleet Division Manager is responsible for monitoring these cards; however, CN4 should review charges incurred by deputies and investigate any unusual charges to help ensure deputies are adhering to all applicable fuel policies.
3. In order to help reduce costs, a policy should be implemented encouraging CN4 employees to use County pumps as their primary source of fuel for CN4 vehicles. The use of other sources of fuel should be limited as much as possible.

Management Response:

#1: Odometers are traced with the sole purpose of tracking for maintenance. This is currently up to the deputy who drives the car to make sure the maintenance happens at the scheduled mileage. The dates and services required are traced by the office and provided to the deputy for him to follow (info is provided by TNR for us to pass to deputies). We do not currently have and do not plan on passing the mileage responsibility to supervision.

#2: We have asked TNR to please let us know if anything non-standard shows up when our cards usage is review so that we can follow up.

#3: This recommendation has been implemented and is currently in our SOP. This was a great recommendation.