

# Travis County Constable Precinct One

## 2016 Inherent Risk Assessment



**TRAVIS COUNTY AUDITOR'S OFFICE**  
Risk Evaluation & Consulting Division

March 10, 2017

TRAVIS COUNTY  
AUDITOR'S OFFICE

NICKI RILEY, CPA  
COUNTY AUDITOR



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

---

To: Danny Thomas  
Travis County Constable, Precinct 1

From: Nicki Riley, CPA  
Travis County Auditor

Date: March 10, 2017

Re: 2016 Risk Assessment

The Risk Evaluation and Consulting Division (REC) of the Travis County Auditor's Office has completed a risk assessment of the Travis County Constable, Precinct 1 (CN1) Office. The objective of the risk assessment was to assist the Constable 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 the identification and rating of risks that are intrinsic to the Constable'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.

Pages 5 through 11 of this report contain a summary of our methods and results. The organizational structure, mission and objectives, significant activities, and financial data for CN1 are then provided on pages 12 through 15. The details of CN1's risk assessment, including the identified business processes, inherent risks, controls implemented by management, inherent risk ratings and area of concerns are provided on pages 16 through 22.

## **BACKGROUND**

---

The Travis County Constables are constitutionally authorized peace officers. They have the same arrest powers and duties as municipal police officers and sheriffs and have the added responsibility of executing civil process for the courts.

The Constable's Office serves as judicial officers for Travis County Courts, including the Justice of Peace Courts, District Courts, and County Courts-at-Law. They are responsible for executing warrants and serving processes that are directed to them, including eviction actions and seizing property. Additionally, they execute civil and criminal processes throughout the county, including citations, notices, warrants, subpoenas, and writs.

As trained Peace Officers, the Constables and their staffs provide County residents the first level of law enforcement protection. Travis County has five Constables directly elected to four-year terms by the residents of their respective precincts. These offices are primarily governed by the Code of Criminal Procedure, the Texas Rules of Civil Procedure, and other applicable laws. Through State statute, Constables are mandated to attend to the Justice of the Peace Courts in their respective precincts, to include providing bailiff services, transporting prisoners, and summoning jurors.

In addition to their judicial and statutory responsibilities, Constables perform various unique law enforcement activities in their precincts. These include traffic law enforcement, special event monitoring, efforts aimed at curbing gang and narcotics activity, involvement with youth programs, a K-9 Unit, bike patrol, lake and park security, and a variety of other functions.

## SCOPE

---

The risk assessment covered the operations of CN1 and was limited to the business processes that were in place during the time the risk assessment was being performed - the three months ending November 30, 2016. 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 CN1 Office.

## ENGAGEMENT TEAM

---

Angel Candelario, Lead Auditor  
Jennifer Bodiker, Staff Auditor

## CLOSING

---

This report is intended solely for the information and use of the CN1 Office, the Auditor's Office and County management as copied below. 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 – Risk  
Evaluation & Consulting



---

Patti Smith, CPA  
First Assistant County Auditor



---

Nicki Riley, 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  
Danny Thomas, Constable, Precinct 1  
Joe Alvarado, Financial Manager, Constable, Precinct 1  
Issac Flynn, Senior Accountant, Constable, Precinct 1  
Gwen Doyle, Office Manager, Constable, Precinct 1  
Frank Stover, Atchley and Associates, CPAs  
Managers, Travis County Auditor's Office

## **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 to rate 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 the Constable's Office, Precinct 1.

### 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 all of CN1 on a five-level scale from very low to very high. A summary of the risk ratings is presented in graph form on page 19 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 CN1, 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 8 of this report. The top two business processes in terms of inherent risk are provided below:

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

# DETAILED REPORT

## RISK ASSESSMENT PROCESS

---

We performed an engagement-level risk assessment of the inherent risks associated with the Travis County Constable, Precinct 1 operations in the following three phases:

<b>DATA GATHERING</b>
-----------------------

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 CN1:

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 (inter-local, professional services, and revenue)
5. Listing of programs
6. Fee schedules
7. Policies and procedures
8. Formally documented narratives and flowcharts

Before meeting with CN1 staff, we reviewed the above documentation, prior audit reports, Texas statutes pertaining to the responsibilities of CN1, 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 Financial Manager, Senior Account, Office Manager, and Constable Sergeant, at their office on Heflin Lane. At this meeting, we provided an explanation of how our office performs risk assessments as well as the anticipated timeline.

We subsequently held meetings with these staff members and others to discuss their operations and business processes in greater detail. During these meetings, the staff 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 the CN1 include the following:

- Accounts Payable
- Cash Handling
- Fixed Assets
- Fleet
- General Ledger
- Purchasing
- Reporting
- Revenue Generation
- Special Revenue

### **POTENTIAL RISKS**

To identify the potential risks that could prevent CN1 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.

CN1'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:

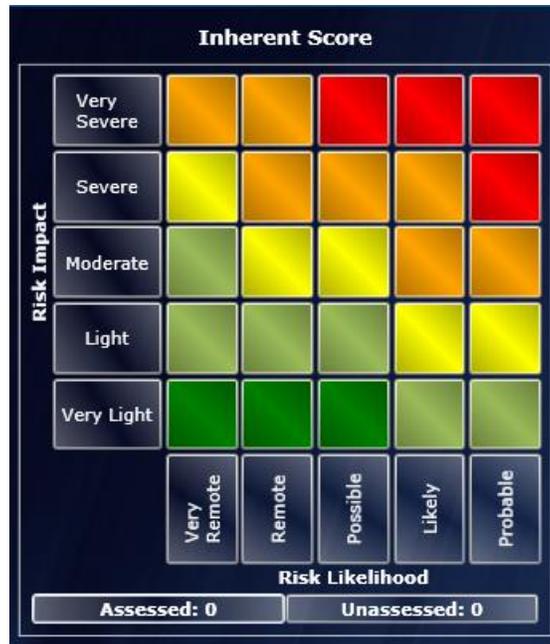
#### IMPACT

- 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:

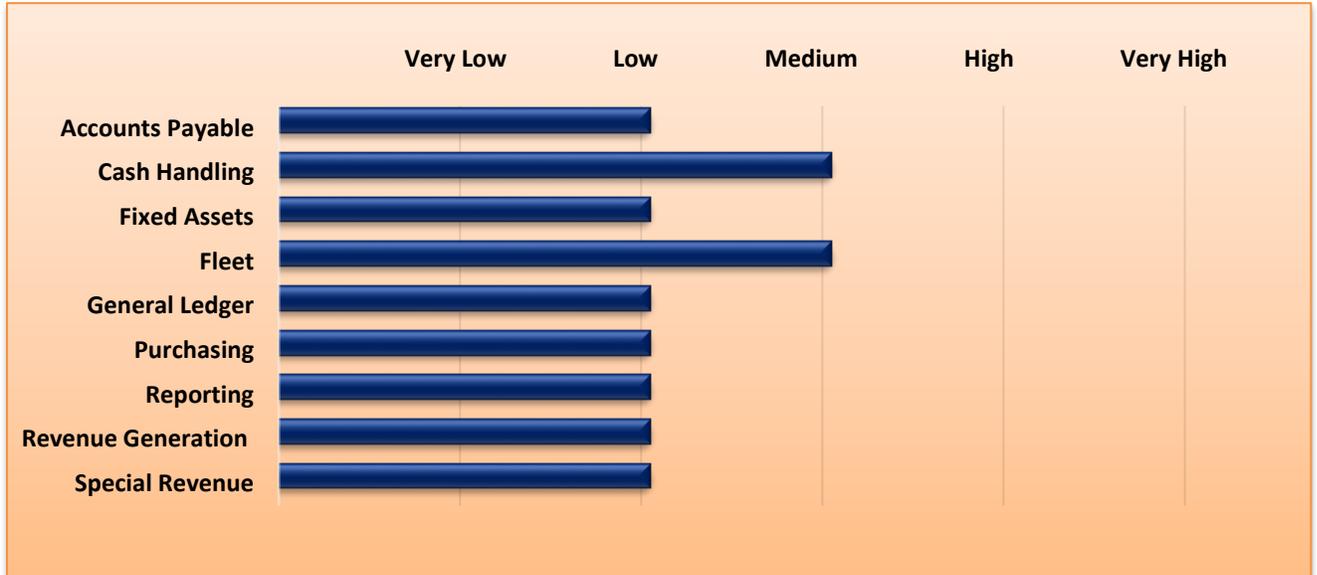
<b>Color</b>	<b>Risk Rating</b>	<b>Description</b>
Dark green	Very low	The risk of loss is remote, or if a loss were to occur, it would have no material impact.
Light Green	Low	The risk of loss is small, and even if a loss were to occur, it would have little material negative impact.
Yellow	Medium	There 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 - RISK PROFILE BY BUSINESS PROCESS

To provide visibility into the business processes which pose the greatest risk to CN1, we present the results in graph form below:



## CONSTABLE, PRECINCT 1, ORGANIZATIONAL CHART

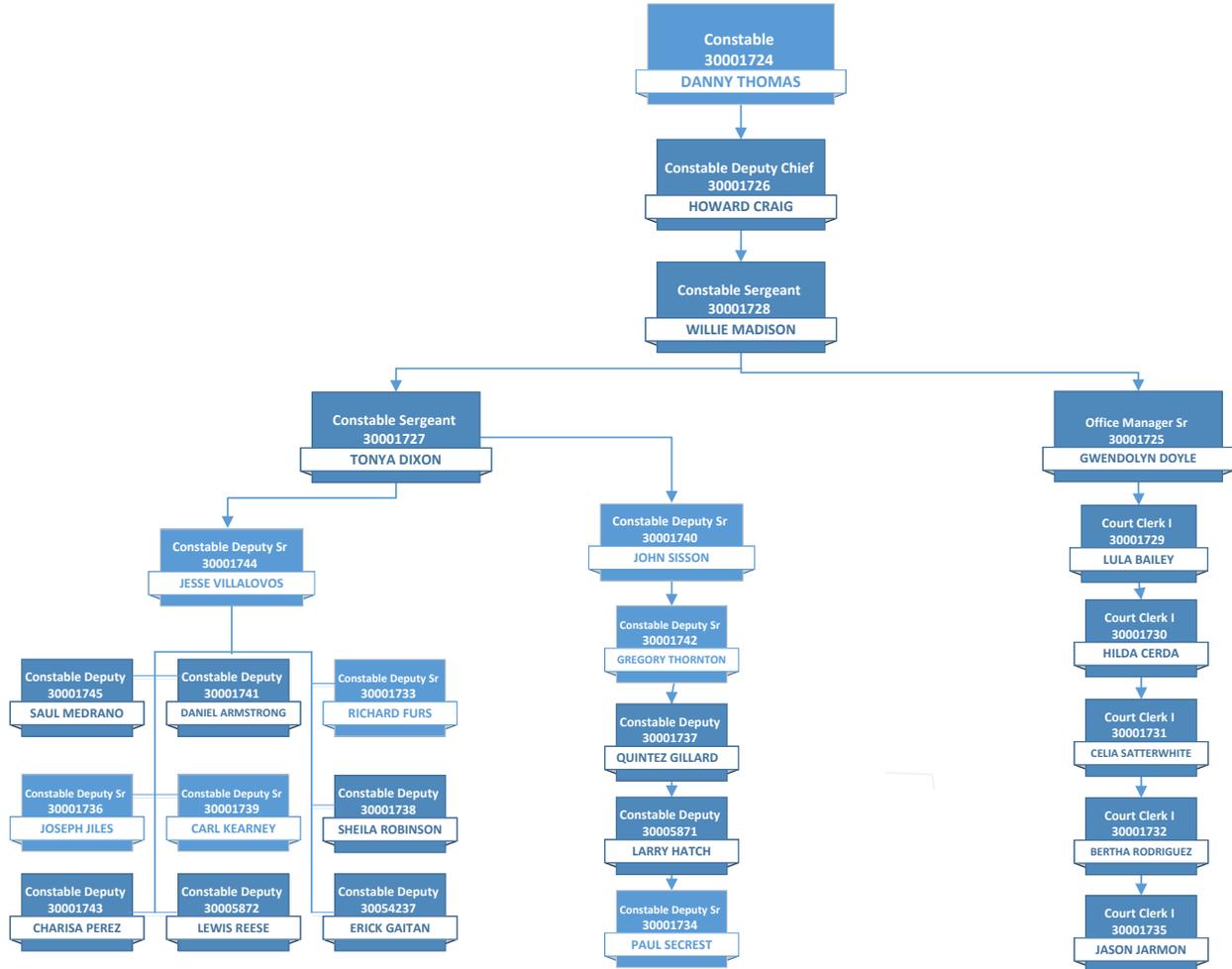


Chart information obtained from SAP – December 2016

Accounting functions for the Constable, Precinct 1 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 CN1 accounting function:

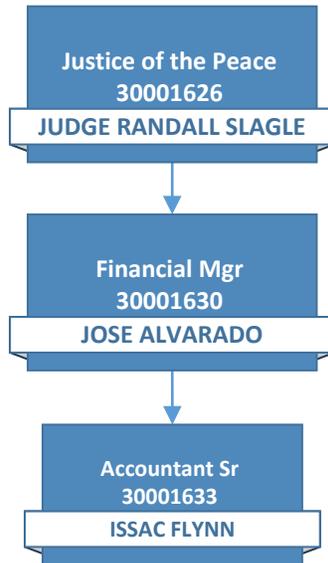
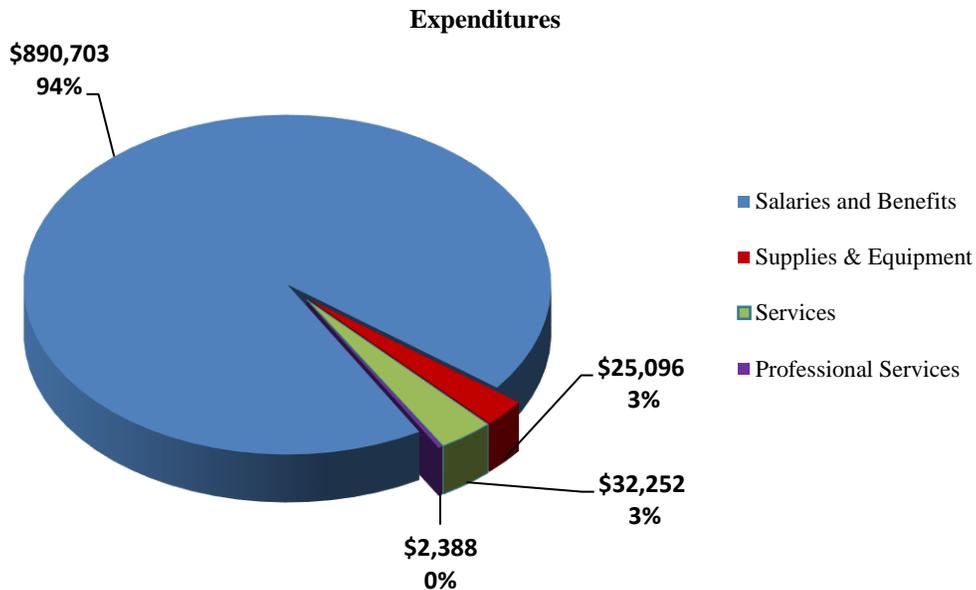
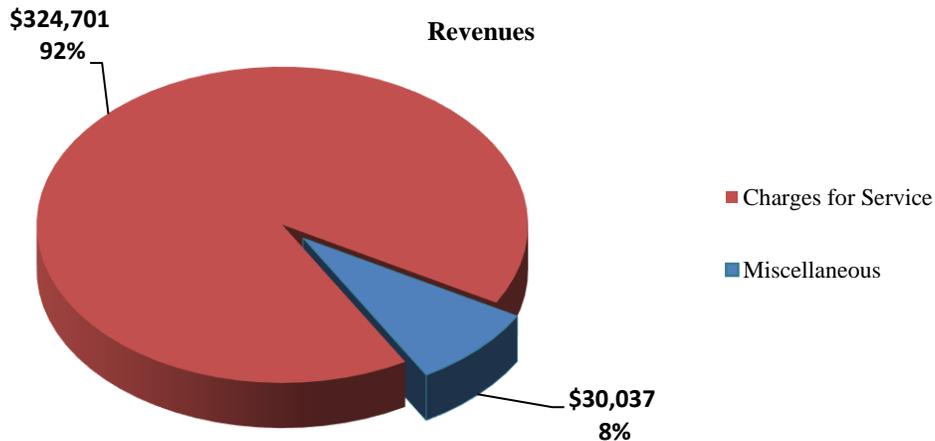


Chart information obtained from SAP – December 2016

## FISCAL YEAR 2016 FINANCIAL DATA

During fiscal year 2016, the Travis County Constable, Precinct 1 received \$324,701 in charges for services and \$30,037 in charges for miscellaneous services, primarily off-duty vehicle use donations. Salaries and Benefits, totaling \$890,703 represented approximately 94 percent of their expenditures. The details for their revenue and expenditures are provided below in graph form:



## **BUSINESS PROCESS RISK PROFILES**

### **MISSION AND OBJECTIVES**

The financial component of the Constable, Precinct 1 Office is responsible for receiving and processing the deposit of collections received both at the office and from field units that collect fines and fees. This component also enters/receipts all assessed fees and off-duty vehicle donations.

In addition, the financial component is also responsible for processing disbursements for refunds, remittance of fees due to the Treasurer (including State Court costs), judgements on writ of executions due to the plaintiff, and escheating unclaimed property. 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, use of Law Enforcement Officer Standards and Education (LEOSE) funds, procurement of goods, court security, fleet usage, and vehicle maintenance. In addition, all warrants and citations are executed by the operational component of the office.

### **SIGNIFICANT ACTIVITIES**

#### **Accounts Payable**

The Senior Accountant processes disbursements, which include refunds for overpayments, execution payments, Treasurer payments, and unclaimed funds to the State and/or Treasurer. Fees due to the Treasurer are remitted via ACH on a daily basis, and financial staff initiates the entry of these deposits into the SAP system. Refunds for overpayments are disbursed weekly. Unclaimed funds that are eligible to be escheated are remitted annually to the State and Treasurer in accordance with Statute guidelines.

#### **Cash Handling**

Court Clerks collect fines and fees already entered into the Odyssey computer system by the Travis County Justice of the Peace, Precinct 1 Office. However, if a party to a civil suit from outside of Precinct 1 wishes to have the CN1 department serve papers to another party, then CN1 will perform the service and enter these collected fees into QuickBooks. The Constable's Office does not serve civil papers unless the fee is paid in advance.

#### **General Ledger**

The Senior Accountant and an Account Associate post journal entries and reconcile the general ledger accounts to the supporting records in QuickBooks and SAP on a monthly basis. The Financial Manager conducts a monthly review on the general ledger accounts.

#### **Bank Reconciliations**

The Senior Accountant completes a weekly and monthly reconciliation of the operating and LEOSE bank accounts. This process includes verifying corrections of any discrepancies were completed, and that all funds collected and disbursed per the office accounting records were received and paid. The Financial Manager performs periodic reviews of monthly reconciliations, which are used in the preparation of the monthly financial statements.

## **Reporting**

On a monthly basis, the Senior Accountant exports system-generated reports, which support the data provided in the financial statements. The Senior Accountant verifies the totals on the financial statements and system-generated reports agree with each other. Upon completion, the financial statements are approved by the Constable and submitted to the County Auditor's Office. Annually, the Financial Manager provides the financial statements for the Comprehensive Annual Financial Report.

## **General Operations**

General Operations is comprised of five separate process areas: fixed assets, fleet, procurement of goods, special revenue fund, and the management of the vehicle donation program.

The Office Manager is responsible for managing fixed assets, procurement of goods and the LEOSE fund. The Officer Manager has also been designated by the Constable as the Purchasing Agent Liaison, which is responsible for the purchasing, receipting, and tagging of new assets, as well as assisting in conducting inventories and maintaining control of fixed assets.

The Office Manager approves all requests for goods. A clerk creates the shopping cart in SAP for the Officer Manager's approval. In addition, the Office Manager is responsible for confirming that vendors are approved, ensuring requests include quotes and other required supporting documents, confirming funds are available, verifying goods are received, and creating goods receipts in SAP for the Auditors Office.

LEOSE funds are allocated by the State Comptroller Office to local law enforcement for the purpose of continuing education. The LEOSE Law Enforcement Fund (SAP Fund #0116) was authorized under Senate Bill 1135. It provides for state moneys to law enforcement agencies to ensure continuing education for persons licensed under Chapter 415, Government Code. Annually, the Office Manager sends the required request forms to the Comptroller requesting LEOSE funds. Upon approval from the Comptroller Office, the funds are sent to CN1 Office and deposited in the LEOSE account. All training requests are sent to the Office Manager and approved by the Constable. The Office Manager is responsible for ensuring training meets LEOSE rules, reviews request packet completeness, verifies funding, provides check for training expense, reconciles settlements, and files packet with all supporting documents.

The Officer Manager is responsible for ensuring the security of confidential file information. Confidential file information is secured in a locked area where only the Office Manager and clerks have access. Employees are required to complete safeguarding confidential information training. The Officer Manager maintains all employees safeguarding confidential information training certificates. Case information is only provided to the person directly involved in a case after proper identification has been provided.

In order for a third party to request information on a case, they must submit an open records request. Below is process for open records requests:

- All open records requests are submitted to the County Attorney for guidance.

- Based on the County Attorney’s guidance, the Court Clerk completes the request.
- A Court Clerk contacts requestor and lets them know if there are fees associated with the request and when they can view the information.
- All requestors must come to the Constable Office to view the information.
- No information is sent via mail, email, etc.
- All information that is released is approved by the County Attorney and Office Manager.

A Constable Sergeant manages the off-duty vehicle donation program. The vehicle donation is an agreement for the use of County vehicles in connection with off-duty employment of County peace officers. This agreement is entered into by a Travis County Constable’s office and an entity requesting support. An entity requests one or more off-duty officers to provide security services/traffic control services, etc. The Constable Sergeant receives these requests and determines that the use of the vehicles will serve a public purpose (conserve the peace, protect life and property, ensure the public safety, etc.). To ensure that the public purpose is met, the Constable Sergeant will at all times retain control over the vehicles.

The entity compensates the off-duty officers directly in accordance with a separate agreement or understanding entered into between the entity and the officers. The entity reimburses the Constable \$20 per hour for use of the County vehicles. The parties agree that such reimbursements shall be deemed a donation to the County under section 81.032 of the Texas Local Government Code.

A Constable Sergeant has been designated by the Constable as the Fleet Manager and is charged with overseeing the fleet. The Fleet Manager is responsible for fleet security, assignment of vehicles, ensuring maintenance is conducted in a timely manner, and managing fuel cards. Officers are assigned vehicles and allowed to drive those vehicles home each day. The officers are also responsible for initiating maintenance and repairs for their assigned vehicles with the TNR Fleet Department.

The Constable is responsible for the building and court-room security. Officers attend court-room security training annually. At the building’s point-of-entry, two officers are required to man the X-ray station. All other building access requires a badge for entry. The building is secured at night. CN1 building is equipped with the following:

- The building has a point-of-entry screening which consists of an X-ray machine and body wand.
- Personnel entering the building must sign in on the visitor roster.
- There are cameras located throughout the interior and exterior of the building.
- There are designated meeting rooms for defendants that are separated from the public, staff, and judicial officers.
  - The Jury room is used for overflow
- The judge has a designated parking space that is not in the main parking lot.
- Plexiglas is installed between the Court Clerks and defendants.
- Constable deputies are required to attend incident response training annually.
- A bailiff is in the court-room at all times when court is in session.

## BUSINESS PROCESS RISKS AND RISK RATINGS

The following chart depicts the risk ratings for the CN1 business areas:

Business Process	Risk Rating
Accounts Payable	Low
Cash Handling	Medium
Fleet	Medium
Fixed Assets	Low
General Ledger	Low
Purchasing	Low
Reporting	Low
Revenue Generation	Low
Special Revenue	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 to prevent loss or misappropriation.
2. Implementation and maintenance of sufficient cash handling and bank reconciliation controls are essential to safeguarding funds from loss or misappropriation.
3. Implementation of an Emergency Action and Recovery Plan to address security breaches, interruptions to daily operations resulting from catastrophic events, and concerns of employee safety.
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 both as needed and at regular intervals, in order 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:

### SECURITY

Building security and employee safety is a critical responsibility of the CN1 Office. Currently, the CN1 Office does not have an incident or emergency response plan in place. We met with the County's Facilities Management Department (FMD) Security Division, and they are in the process of implementing a County Emergency Response and Preparedness Plan and 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.

We recommend that, at a minimum, policies and procedures be established to address courtroom security and incident response plans. CN1 should initiate an interim plan until the FMD Security Division is able to evaluate the site and assist with implementation of an emergency response plan. We recommend that the CN1 office coordinate with FMD to determine when their building is scheduled for an assessment. Upon completion of the assessment, CN1 should review the assessment and work closely with FMD to implement the plan.

Currently, there is no trained/qualified staff member to support clients with physical and psychiatric needs. Instead, CN1 coordinates with Austin Police Department for support. CN1 should evaluate the need for a trained person on staff to handle physical and psychiatric needs clients.

### FLEET

There is not a system in place to manage fuel cards. Fuel cards are not secured while not in use, with active fuel cards residing in an unlocked desk. On occasion, fuel cards are issued without being logged out. We recommend that an accountability system be implemented to manage this issue and prevent the loss/theft of these cards.

The Fleet Manager was unable to provide a list of assigned vehicles by officer. In SAP, the majority of vehicles are assigned to the Fleet Manager. A list of vehicle assignments has not been provided to the County Risk Management office. According to County Policy Chapter 40.002(e)(3)(A) & (B), CN1 is required to provide a list of this type to the Risk Management office. We recommend that the Fleet Manager assign all vehicles to officers through SAP, and conduct a periodic review to ensure the proper vehicles are assigned to their respective officer. In addition, CN1 should provide a copy of the accurate vehicle assignment list to Risk Management.

During the risk assessment, we noted that there were no written rules for off-duty fleet, and according to Travis County Code Chapter 40.002(d), CN1 is required to provide these rules to the Auditor's Office and Risk Management. This Code section requires that these rules include the items on the following page:

*“(1) whether and under what circumstances the employee may use a county-owned passenger vehicle to accomplish personal errands,  
(2) whether and under what circumstances the employee may use a county-owned passenger vehicle to travel to or from a place of employment other than employment with Travis County,  
(3) whether an employee may use a county-owned passenger vehicle for other employment while off-duty and, if so, the type of employment for which it may be used, and  
(4) whether and under what circumstances the employee may allow any other person to drive or to occupy a county-owned passenger vehicle.”*

We recommend that the Fleet Manager establish written rules for off-duty fleet to help prevent the misuse of county vehicles, providing a copy of these rules to the Auditor’s Office and Risk Management when completed.

### **FIXED ASSETS**

Travis County fixed asset policies and procedures can be found in Chapter 32, Subsection W of the Travis County Code. Specifically, Section 32.351 “User Department Responsibilities” details the requirements for purchasing, renting/leasing, transferring, disposing, and retiring fixed assets. It also requires an annual physical inventory of all assets assigned to the applicable office. These inventories help ensure that the fixed asset listing is accurate, that office fixed assets are safeguarded, and that Office personnel are accountable for these items.

At the time of the risk assessment, we noted there were no written policies or procedures in place for fixed assets, included a requirement that all Office fixed assets be physically verified on a periodic basis. We recommend this this Office compose and implement fixed asset policies and procedures in agreement with Chapter 32, Subsection W of the Travis County Code.

### **CASH HANDLING**

Customers are allowed to pay with a third-party credit/debit card with the only prompted authorization being the billing zip code. We recommend that the cardholder be present or complete an authorization form allowing charges to be placed on their card on behalf of client.

According to CN1 Cash Handling Procedures, two clerks are to jointly handle and record all funds received through the mail; however, only one clerk currently performs these duties. We recommend that the Office’s cash handling procedures be enforced, and that two clerks jointly handle and record all funds received in the mail. If this is not possible, a compensating control should be implemented, such as a managerial review and verification of these collections.

Clerks preparing the daily deposits also can post, void, and adjust cash receipts in QuickBooks. We recommend that these duties be separated to avoid improper segregation of duties. If this is not possible, we recommend establishing a managerial review process to verify that parties performing daily deposits have not inappropriately created, adjusted, or voided QuickBooks receipts.

## **GENERAL LEDGER**

Currently, there is no managerial review or approval process prior to posting journal entries in QuickBooks. Staff are authorized to post journal entries via rights and roles. We recommend that managers implement a review and approval process prior to journal entries being posted to reduce the potential for error.