

Travis County Auditor's Office  
Risk Assessment Review  
of Travis County Constable, Precinct 5  
September

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: Constable Carlos Lopez  
Constable, Precinct 5

From: Nicki Riley, CPA  
Travis County Auditor

Date: September 5, 2018

Re: 2018 Risk Assessment – Constable, Precinct 5

The Risk Evaluation and Consulting Division (REC) of the Travis County Auditor's Office has completed a risk assessment of the Constable, Precinct 5 (CN5) Office. The objective of the risk assessment was to assist CN5 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 CN5'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, mission and objectives, significant activities, and financial data for CN5 are provided on pages 9 through 14. The details of the office's risk assessment, including the identified business processes, inherent risks and ratings, and areas of concern are provided on pages 15 through 17.

## **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 CN5 and was limited to the business processes that were in place during the time the risk assessment was being performed - the three months ending March 31, 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 CN5 Office.

## **ENGAGEMENT TEAM**

---

Amanda Muehlberg, CPA, Lead Auditor  
Joshua Kubiak, CPA, Staff Auditor  
Travis Lee, Staff Auditor

## **CLOSING**

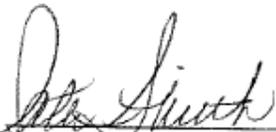
---

This report is intended solely for the information and use of the CN5 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 Jungeman, 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  
Cinda Kortan, Office Manager Senior, Constable, Pct. 5  
Joe Alvarado, Financial Manager, Constable, Pct. 5  
Frank Stover, Atchley and Associates, CPA's  
Managers, Travis County Auditor's Office  
Travis County Executive Managers

## 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. These efforts could include 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 5.

## 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 CN5 on a five-level scale from very low to very high. To provide visibility into the business processes which pose the greatest risk to CN5, we calculated the average risk rating for each business process. The top five business processes in terms of inherent risk are provided below.

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

## DETAILED REPORT

### RISK ASSESSMENT PROCESS

---

We performed an engagement-level risk assessment of the inherent risks associated with the Travis County Constable, Precinct 5 operations in the following three phases:

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

In order to perform an accurate and thorough risk assessment, the auditor first becomes familiar with the nature of the entity's business activities. To begin this process, we requested the following documents from CN5:

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 CN5 employees, we reviewed the above documentation; department website; prior audit reports; Texas statutes pertaining to the responsibilities of CN5; guidance provided by regulatory agencies such as the Office of Court Administration (OCA); various narratives; Commissioners Court Agendas, Backup Support, and Minutes; the Travis County Code; and the Comprehensive Annual Financial Report (CAFR).

At the entrance conference, we met with the Office Manager Senior at the precinct office located in the Holt Building on Guadalupe. 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 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 12 of the 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 CN5 include the following:

- Accounts Payable
- Accounts Receivable
- Cash Handling
- Disabled Parking Enforcement
- Facilities
- Fixed Assets
- Fleet
- General Ledger
- Interlocal Agreements
- Inventory
- Reporting
- Revenue Generation
- Seized Property

### **POTENTIAL RISKS**

To identify the potential risks that could prevent CN5 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 CN5's staff and management appear 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:

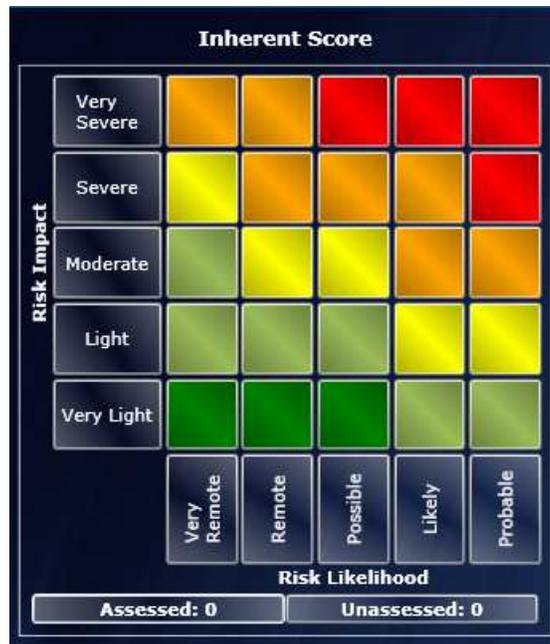
#### IMPACT

- 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.



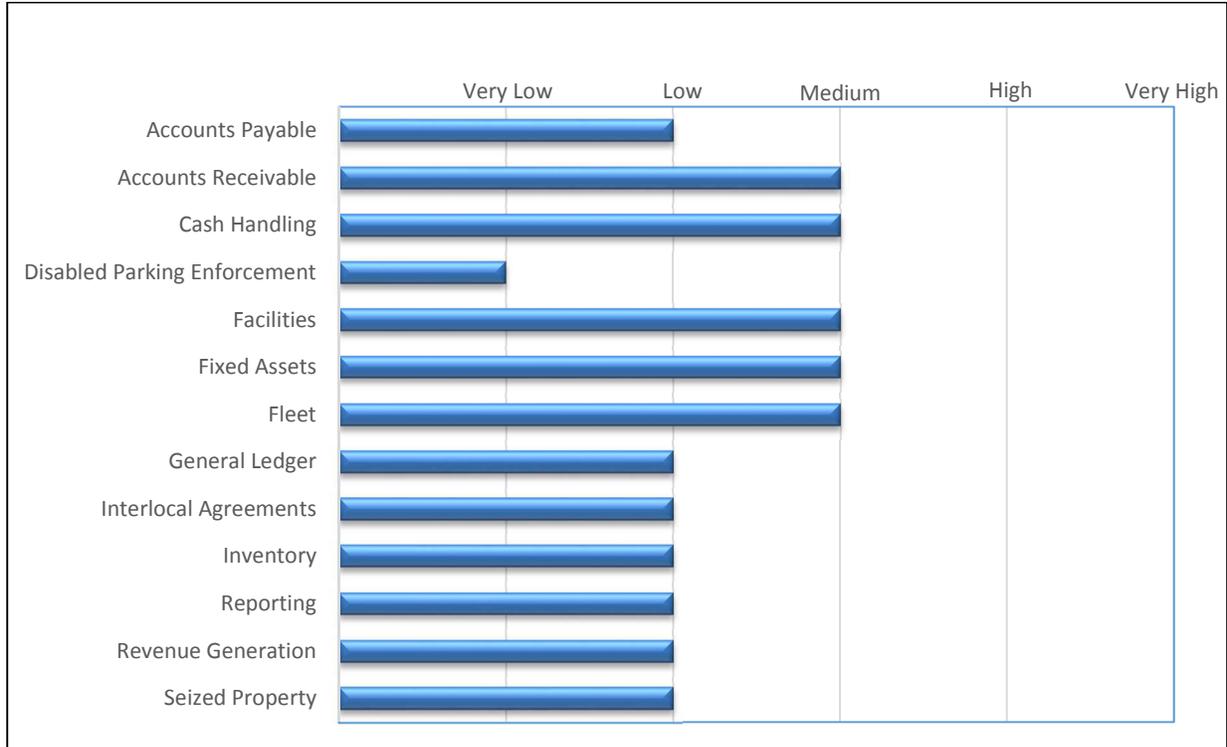
Using this matrix, the inherent risk for each business process was rated on a five-level scale as follows:

<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.

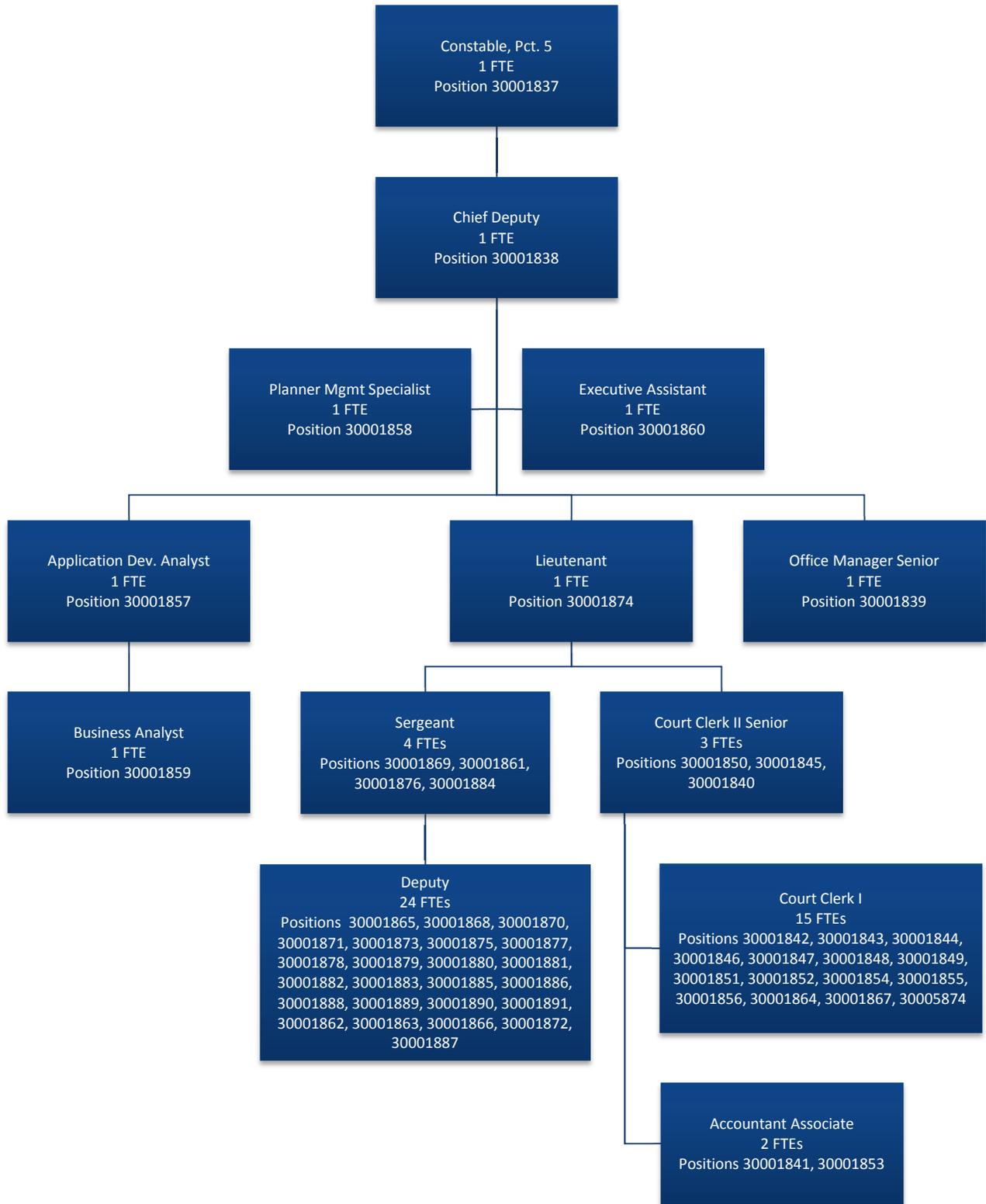
## SUMMARY OF RESULTS

### GRAPH 1 – RISK PROFILE BY BUSINESS PROCESS

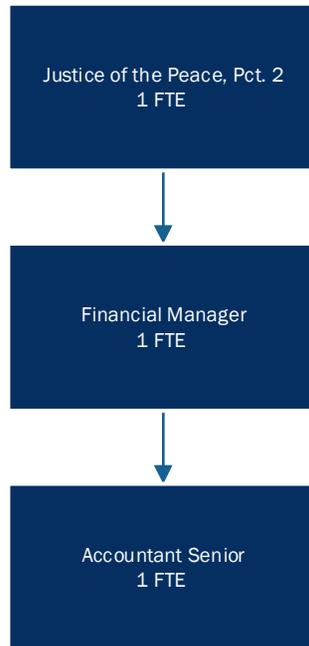
To provide visibility into the business processes which pose the greatest risk to CN5, we present the results in graph form below:



## CONSTABLE, PRECINCT 5 ORGANIZATIONAL CHARTS



Accounting functions for the Constable, Precinct 5 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 CN5 accounting function:

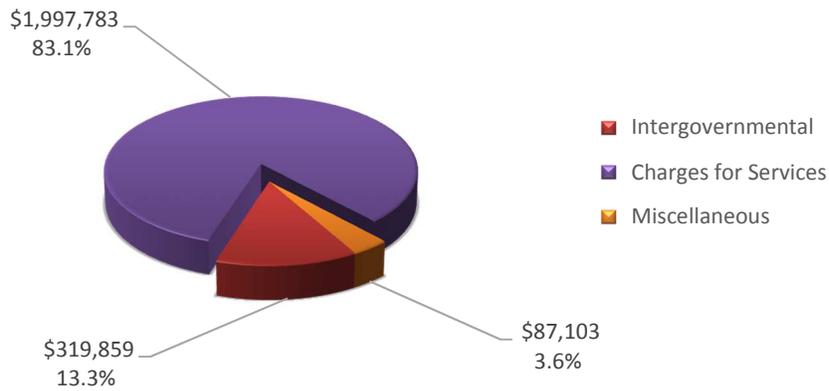


Organizational chart information is as of March 2018

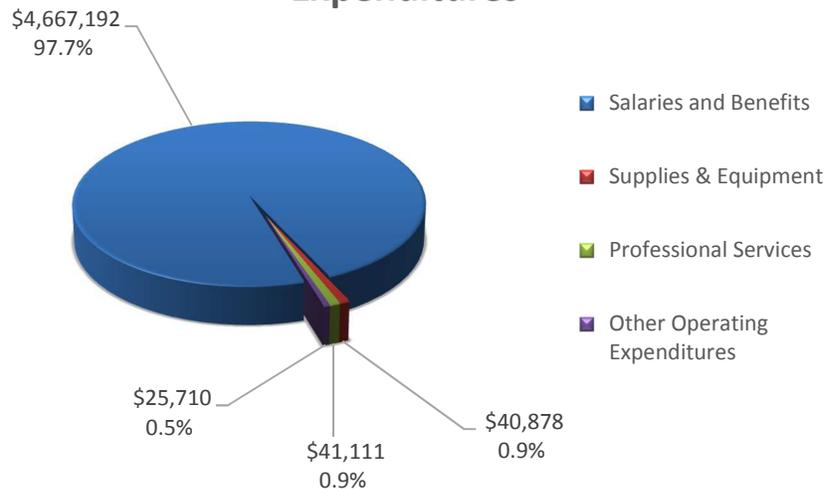
## FISCAL YEAR 2017 FINANCIAL DATA

During fiscal year 2017, the Travis County Constable, Precinct 5 received \$1,997,783 in charges for services, \$319,859 in intergovernmental revenue, and \$87,103 in miscellaneous income. Salaries and Benefits, totaling \$4,667,192 represented approximately 98 percent of their expenditures. The details for their revenue and expenditures are provided below in graph form.

### Revenues



### Expenditures



## **BUSINESS PROCESS RISK PROFILES**

### **MISSION AND OBJECTIVES**

Constable 5 financial personnel are responsible for receiving and processing the deposit of collections received both at the office and from field units that collect fines and fees. These parties also enter/receipt all assessed fees, vehicle donations, and interlocal payments.

This division is also responsible for processing disbursements relating to warrant work by other counties, refunding overpayments, escheating unclaimed property, and posting collections on executions. It also remits 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.

Office administrative personnel are responsible for managing/monitoring fixed assets, inventory stock, facility work orders, fleet usage, vehicle maintenance, and execution of warrants and citations.

### **SIGNIFICANT ACTIVITIES**

#### **Accounts Payable**

Disbursements processed by a lead staff member include refunds for overpayments, fines and fees due to the Justice of the Peace, Precinct 5 (JP5) Office and other governmental agencies, writ of executions, and unclaimed funds remitted to the State and/or Treasurer.

Fees due to the Treasurer and JP5 office are remitted via ACH on a daily basis and financial staff initiate the entry of these deposits into the SAP system. Fees due to other governmental agencies are remitted via check and refunds for overpayments are disbursed as needed. Finally, unclaimed funds that are eligible to be escheated are remitted annually to the State and Treasurer.

#### **Accounts Receivable**

Accounts receivable for CN5 are primarily a result of tax suit filings (both from Travis County and Out of County) that are served by the office. Other items that create a receivable include Attorney General (AG) warrants executed, Out-of-County AG papers, insufficient funds payments, and fees for services provided to legal firms and individuals. In order to review receivables, office personnel create and review an aging report on a monthly basis.

#### **Cash Handling**

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

#### **Disabled Parking Enforcement**

Disabled Parking Enforcement (DPE) is a program that enforces disabled parking laws and issues citations in the event of a violation. Volunteers trained by the CN5 Office issue manual citations for violations. Volunteer training includes an application; criminal background check (applicants with Class B or higher felonies are not allowed to volunteer); signed acknowledgement of policies, procedures, and expectations; and training on judgement and issuance of citations.

Currently, there are 92 active volunteers. Volunteers are able to issue citations for parking in an accessible space without a placard or plate, blocking access to an accessible space or obstructing a ramp, or expired placards. Deputies are the only individuals authorized to issue citations for illegal use of a placard or an altered placard. This is due to the fact that in order to verify illegal use or alteration of a placard, the identification of the person must be determined and volunteers are not able to legally request identification.

### **General Ledger**

On a monthly basis, a lead staff member reconciles the QuickBooks general ledger accounts to the supporting records, posting QuickBooks 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 staff member performs month-end bank reconciliations in order to verify that the weekly reconciliations are accurate and any discrepancies have been corrected in a timely manner. These monthly reconciliations are also used in the preparation of the monthly financial statements.

### **Reporting**

A lead staff member reviews system-generated reports (including reports from FACTS and Odyssey), 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. For risk analysis purposes, employee safety and building security is considered under the purview of facilities. The Chief Deputy oversees the vehicle design needs of the fleet function and creates a vehicle specifications sheet when new vehicles are approved in the budget. Once a vehicle has been purchased and all necessary specialized equipment has been installed, the completed vehicle is delivered to the East Service Center for final approval by the TNR Fleet Division Manager.

While vehicle maintenance is the responsibility of the deputy assigned to the vehicle, it is reviewed and monitored by the Constable Sergeants of each respective unit. The office adheres to County policy when transfer or disposal is necessary. All paperwork is completed and approved by the Chief Deputy prior to the vehicle being removed from CN5's fleet.

The Division Managers are responsible for overseeing facilities and inventory functions for their respective divisions, which include managing work orders; ordering, tagging, and tracking fixed assets; and ordering and monitoring inventory (primarily office supplies).

The Business Analyst Associate is responsible for processing and tracking all fixed assets for the office. In addition, the Business Analyst Associate is the liaison between the CN5 Office and the Purchasing Department for the annual fixed asset verification process.

In January, the CN5 Chief Deputy presented a status report to The Travis County Court Security Committee which indicated that each constable's office has different levels of security for each

facility and there are no current standards for building design, security screening and surveillance equipment, security measures, staffing, or response to critical incidents.

In March, the Facilities Department presented to the Court Security Committee regarding a consultant's report of the security status of several buildings, which included constable's offices. The report had several improvement recommendations (including Holt Building, which houses CN5) and the Facilities Department is working with the Commissioners Court to obtain funding.

The CN5 Office has internal emergency preparedness and security procedures which are reviewed by senior staff and shared with administrative staff. However, they are not presently documented into policy form. CN5 is also looking at the consultant's improvement recommendations and timeline for those improvements to the office space as they expect it will have a direct impact on revision and implementation of current internal security and preparedness processes and policies. They have also reached out to the Facilities Security Division to propose some policies and training for their staff in order to be more consistent with County initiatives, which would also be included in future CN5 policies and procedures.

## BUSINESS PROCESS RISKS AND RISK RATINGS

The following chart depicts the risk ratings for the Constable, Precinct 5 business areas:

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

The following are the primary risk areas/control objectives for this office, which are each associated with medium-rated business processes in the above chart:

1. Receivables are properly tracked, reviewed, and accounted for to ensure accurate account balances and financials.
2. 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 implemented to address security breaches, interruptions to daily operations resulting from catastrophic events, and concerns for 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 at regular intervals to prevent vehicle downtime.

## **AREAS OF CONCERN**

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

### **Accounts Payable**

Currently, disbursements above a certain dollar amount do not require dual signatures. We recommend any disbursements above \$5,000 require two signatures from office management.

### **Accounts Receivable**

1. Receivables are not created for uncollected off-duty vehicle donations. We recommend that receivables be recorded and tracked for these items.
  
2. The collection of citation service revenue is tracked by the District Clerk and Constable 5 in separate systems, FACTS and CN5's internal tacking system respectively. Citation fees receivable are not tracked in a consistent manner in the two systems, and a periodic reconciliation of the two systems is not performed. Upon noting this, we reviewed civil citations for 19 cases for which payments were received in the period January 1, 2018 to February 28, 2018. This review disclosed the following:
  1. For one case (Cause #D-1-AG-12-000393), the District Clerk (DC) issued three citations - one by private service and two by CN5 for \$70 each. CN5 records show four citations issued - three for \$70 and one for \$75.
  2. For one case (Cause #D-1-AG-09-001009), CN5 listed four issued citations - two for \$70 each and two for \$75 each. DC records also showed four citations issued; however, two were sent to private services and the remaining two were sent to CN5 at \$75 each.
  3. For one case (Cause #D-1-FM-99-007217), CN5 issued two citations that should have been billed for \$70 each. The DC recorded four – two in 2006 for \$60 each and two in 2013 for \$70 each.
  4. One citation fee assessment resulted in a duplicate payment that was noticed by the customer and has since been reimbursed. However, the lack of a clear reconciliation between DC and CN5 records suggests this would not have been discovered by either office.

Due to the lack of reconciliation between the two systems, CN5 is unable to verify that the proper payments are being received for all civil citations served. We recommend the CN5 Office coordinate with the District Clerk's Office to perform this reconciliation regularly.

### **Cash Handling**

1. For funds received in the mail, the employees that open the mail and complete the mail log have access to create system-generated receipts. In addition, checks received in the mail are not logged until the following business day. A second employee does not consistently act as a witness to the opening of the mail and creation of the mail log and an independent review is not performed to verify that all mailed-in payments have been deposited. We recommend the implementation of

controls to improve these processes including logging all payments received in the mail on the day of receipt.

2. Office policy requires that employees preparing daily deposits do not collect and receipt funds; however, these parties have access to create system-generated receipts. We recommend that office management periodically verify that parties performing daily deposits have not created, adjusted, or voided receipts for funds collected.
3. Parties making payments on balances due using credit and debit cards are not required to present formal identification. Because of this, these parties could use a credit or debit card that is not in their name to make a payment. We recommend that for debit/credit card transactions, office personnel verify that the cardholder name matches either the payor's ID or the applicable case information.
4. Funds that are not deposited prior to the end of a business day are kept in a locked office or locked file drawer. The keys to access these two areas are accessible by all CN5 employees. We recommend that the office obtain a safe in which to store funds collected until they can be deposited. Only the appropriate members of office management with no cash handling responsibilities should have access to the safe combination/keys.

### **Facilities**

All deputies are issued fuel cards for their vehicles. The TNR Fleet Division Manager is responsible for monitoring these cards; however, CN5 should review charges incurred by deputies and investigate any unusual charges to help ensure deputies are adhering to all applicable fuel policies.

Although the office has an emergency response plan that is communicated to staff, it does not have a documented emergency response plan that employees are able to reference. We recommend the current plan be formally documented and be distributed to all office personnel. We also recommend that the CN5 Office work with other constable offices to determine best practices for emergency preparedness and employee safety.