

Travis County Justice of the Peace, Precinct 4

2016 Inherent Risk Assessment

TRAVIS COUNTY AUDITOR'S OFFICE
Risk Evaluation & Consulting Division

April 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: Judge Raúl Arturo González
Justice of the Peace, Precinct 4

From: Nicki Riley, CPA
Travis County Auditor

Date: April 10, 2017

Re: 2016 Risk Assessment – Justice of the Peace, Precinct 4

The Risk Evaluation and Consulting Division (REC) of the Travis County Auditor's Office has completed a risk assessment of the Justice of the Peace, Precinct 4 (JP4) Office. The objective of the risk assessment was to assist JP4 in identifying potential risks or exposures associated with their business processes, allowing them to implement or adjust internal controls as they deemed necessary.

An engagement-level inherent risk assessment was performed to focus on identifying and rating risks that are intrinsic to JP4's activities and business processes. To a limited extent, we considered the impact of internal controls implemented by management to mitigate these risks. Furthermore, 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.

An executive summary is provided starting on page 2.

BACKGROUND

The Justice of the Peace presides over the Justice Court and Small Claims Court. The Justice of the Peace also sits as magistrate for juvenile warnings, felony warrants, and examining trials. The Court's jurisdiction includes civil disputes and small claims of \$10,000 or less, criminal cases on Class C misdemeanors of \$500 or less, and sanction power on certain Class C cases (alcohol, tobacco, and education codes). Class C misdemeanor cases include traffic violations, minors in possession of alcohol, and disorderly conduct.

The Justice of the Peace handles forcible detainers (evictions), driver's license suspension hearings, animal cruelty cases, disposition of stolen property matters, and nuisance cases. The Justice of the Peace also presides over hearings on deed restrictions and performs marriage ceremonies.

JP4 is responsible for the collection of court fees, issuance of warrants, various types of civil processes, issuance of summonses, assignment and monitoring of community service, and monitoring compliance of mandatory drug and alcohol rehabilitation classes. Furthermore, the Justice of the Peace conducts peace bond hearings, reviews applications for mental health or chemically dependent commitments, conducts compulsory school attendance trials, and gives warnings required by law to juveniles.

SCOPE

The risk assessment covered the operations of JP4 and was limited to the business processes that were in place during the time the risk assessment was being performed - the four months ending December 31, 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 JP4 Office.

ENGAGEMENT TEAM

John Gomez, Lead Auditor
Camille Cortez, Staff Auditor
Jennifer Bodiker, Staff Auditor

CLOSING

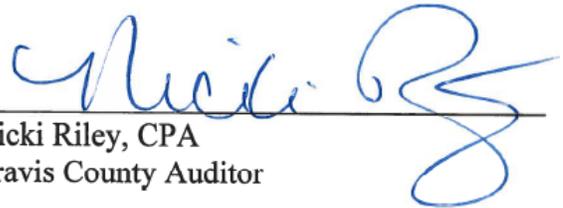
This report is intended solely for the information and use of the JP4 Office, the Auditor's Office, and County management. We greatly appreciate the cooperation and assistance received from management and staff during this risk assessment. Please contact our office if you have any concerns or questions regarding this report.



David Jungerman, CIA
Chief Assistant County Auditor – 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
Diana Cantu, Court Administrator, Justice of the Peace, Pct. 4
Joe Alvarado, Financial Manager, Justice of the Peace, Pct. 2
Frank Stover, Atchley and Associates, CPA's
Executive Managers
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 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, a numeric value is assigned 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?

Risk assessments performed by the Auditor's Office are used to allocate audit resources to areas with the 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.

TABLE OF CONTENTS

Transmittal Letter	i
Introduction to the Risk Assessment Report Format	iv
Executive Summary	2
Purpose	2
Methodology	2
High Risk Areas.....	3
Detailed Report.....	4
Risk Assessment Process	4
Data Gathering	4
Identification of Business Processes, Risks, and Controls.....	5
Rate Inherent Risks.....	6
Summary of Results	8
Graph 1 – Risk Profile by Business Process	8
Justice of the Peace, Precinct 4 Organizational Chart	9
Fiscal Year 2016 Financial Data	10
Business Process Risk Profiles	11
Mission and Objectives.....	11
Significant Activities	11
Business Process Risks and Risk Ratings.....	15
Areas of Concern	16
Cash Handling	16
IT & Information Systems.....	16
Facilities.....	17

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. There are two levels of risk assessments: Enterprise and Audit/Engagement.

ENTERPRISE RISK ASSESSMENT (ERA)

An enterprise 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. The three types of risks (Inherent, Control, and Residual) are identified, evaluated, and rated when performing an ARA.

- **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, only the inherent risks will be rated 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 JP4 Office.

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

The risks inherent to the business processes handled by all of JP4 were rated on a five-level scale from very low to very high. A summary of the risk ratings is presented in the Risk Rating Description Table on page 7.

BUSINESS PROCESSES

To provide visibility into the business processes which pose the greatest risk to JP4, we calculated the average risk rating for each business process. A summary of the average risk ratings for the business processes is presented in the Risk Profile by Business Process graph (Graph 1) on page 8 of this report. The top three business processes in terms of inherent risk are provided below:

<u>Business Process</u>	<u>Risk Rating</u>
Cash Handling	Medium
Facilities	Medium
IT & Information Systems	Medium

The inherent risks, risk management techniques, and risk ratings for the business processes are provided in detail in the Business Process Risk Profiles section beginning on page 11 of this report.

DETAILED REPORT

RISK ASSESSMENT PROCESS

The engagement-level risk assessment of the inherent risks associated with the Travis County Justice of the Peace, Precinct 4 operations was performed in three phases: data gathering; business process, risk, and control identification; and risk rating.

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, the auditor requested the following documents from JP4:

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. Listing of programs
4. Fee schedules
5. Policies and procedures
6. Formally documented narratives and flowcharts
7. The Travis County Justice of the Peace, Precinct 4 web page (<https://www.traviscountytx.gov/justices-of-peace/jp4>)

Before meeting with the JP4 employees, we reviewed the above documentation, prior audit reports, Texas statutes pertaining to the responsibilities of JP4, guidance provided by regulatory agencies such as the Office of Court Administration (OCA), various narratives, Commissioners Court Agendas, Backup Support/Minutes, Travis County Code, and the Comprehensive Annual Financial Report (CAFR).

At the entrance conference, the auditors met with the Court Administrator, Accounting Manager, and Business Analyst at their office located on McKinney Falls Parkway. At this meeting the auditors provided an explanation of how the risk assessment will be performed, as well as the anticipated timeline.

We later held meetings with the Court Administrator, Accounting Manager, and Senior Court Clerks, obtaining a high-level overview of their operations. We subsequently held meetings with 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 11 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 these 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, revenue generation, etc. Business processes in place at JP4 include the following:

- Accounts Payable
- Cash Handling
- Court Functions
- Facilities
- Fixed Assets
- General Ledger
- Inventory
- IT & Information Systems
- Reporting
- Revenue Generation

POTENTIAL RISKS

To identify the potential risks that could prevent JP4 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 these 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 assessments, 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. Management control is not a factor in determining the level of inherent risk, nor does a high degree of inherent risk 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 JP4'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

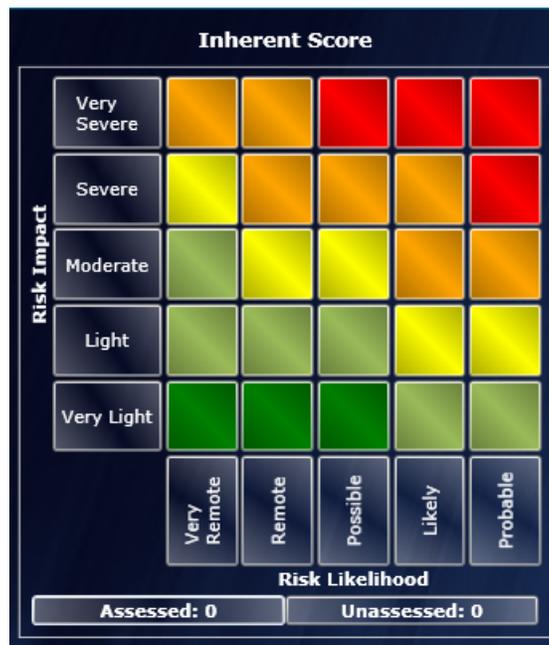
- Volume/dollar value/operational significance
- Media attention
- Government regulation
- Damage to customers or third parties
- Data privacy and protection

LIKELIHOOD

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

Adjustments were made based on auditor judgment and other factors as was deemed appropriate.

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:

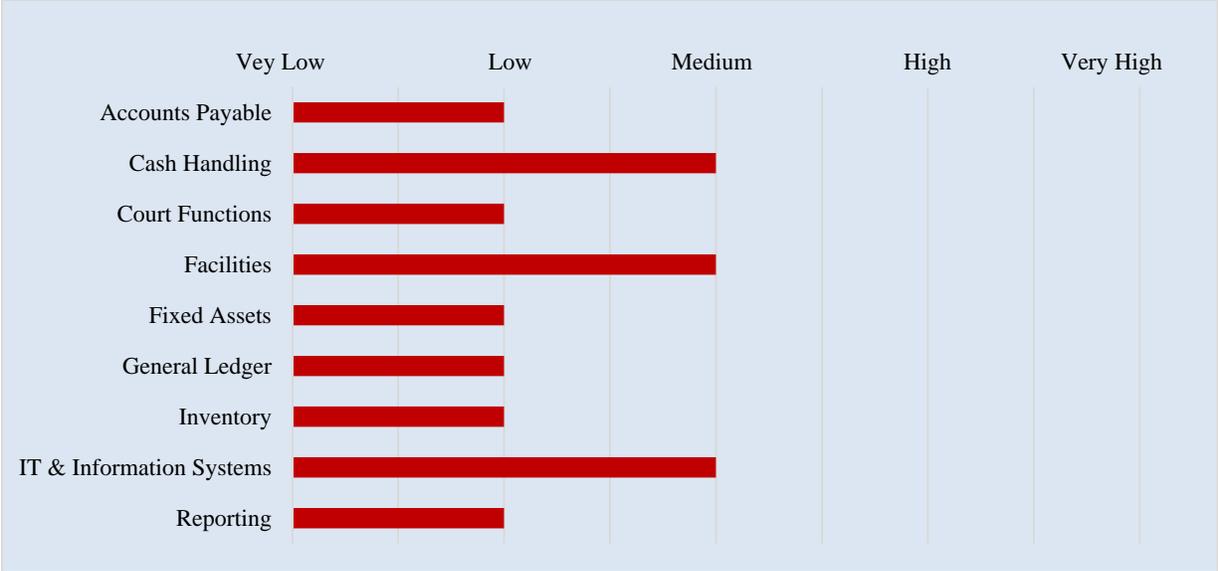
TABLE 1: RISK RATING DESCRIPTION

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

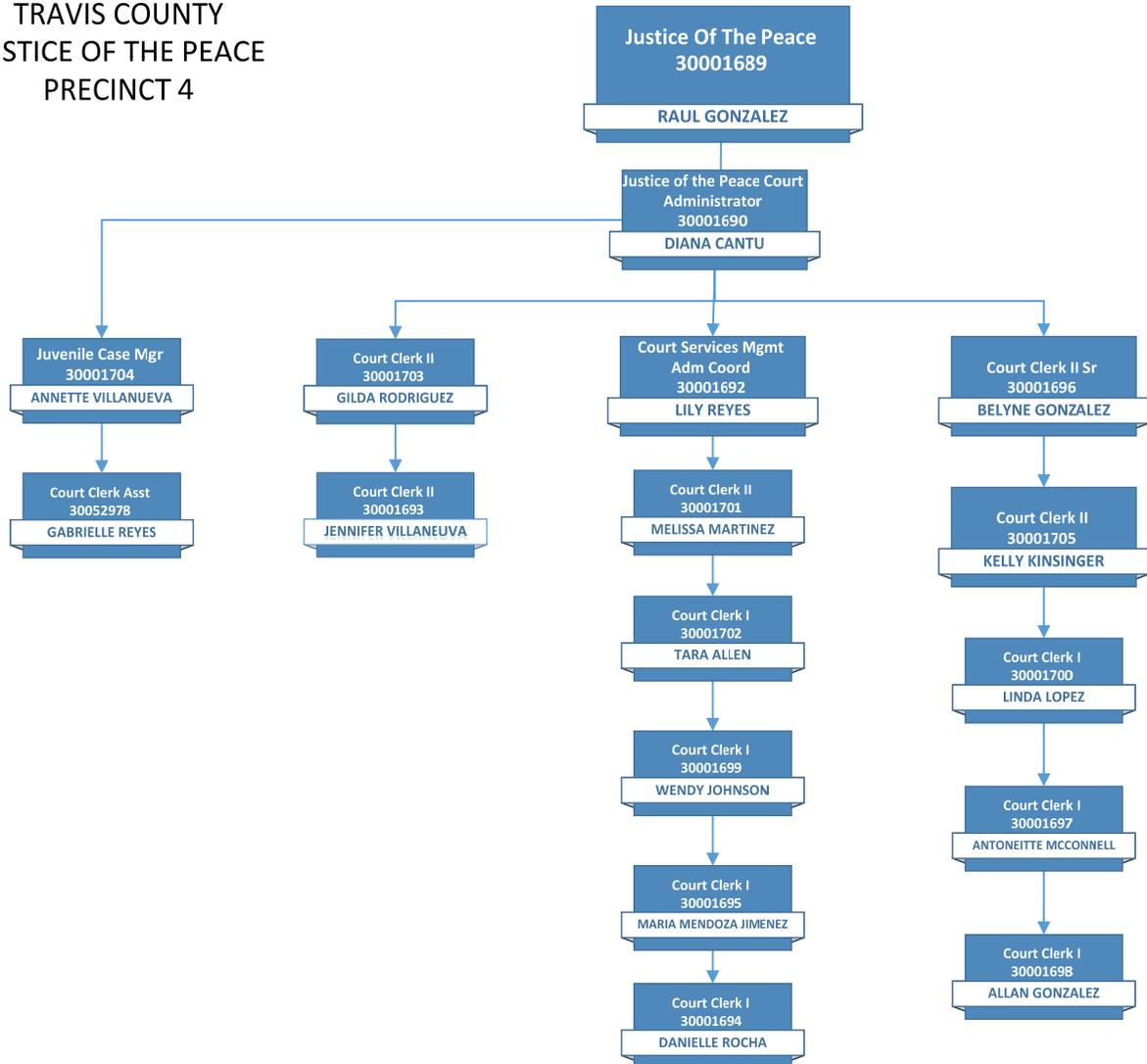
GRAPH 1 – RISK PROFILE BY BUSINESS PROCESS

To provide visibility into the business processes which pose the greatest risk to JP4, we present the results in graph form below:



JUSTICE OF THE PEACE PRECINCT 4 ORGANIZATIONAL CHART

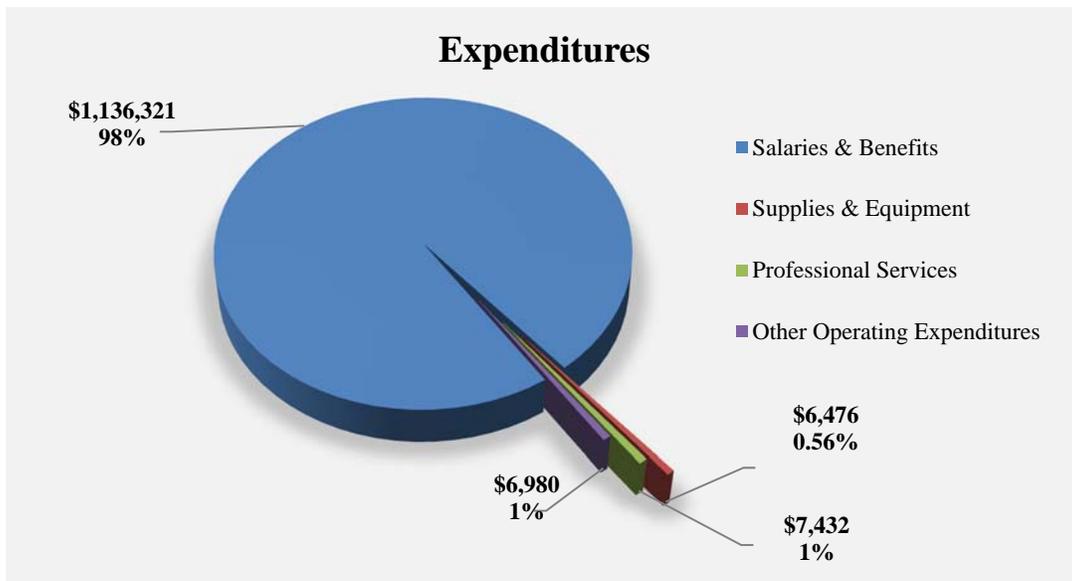
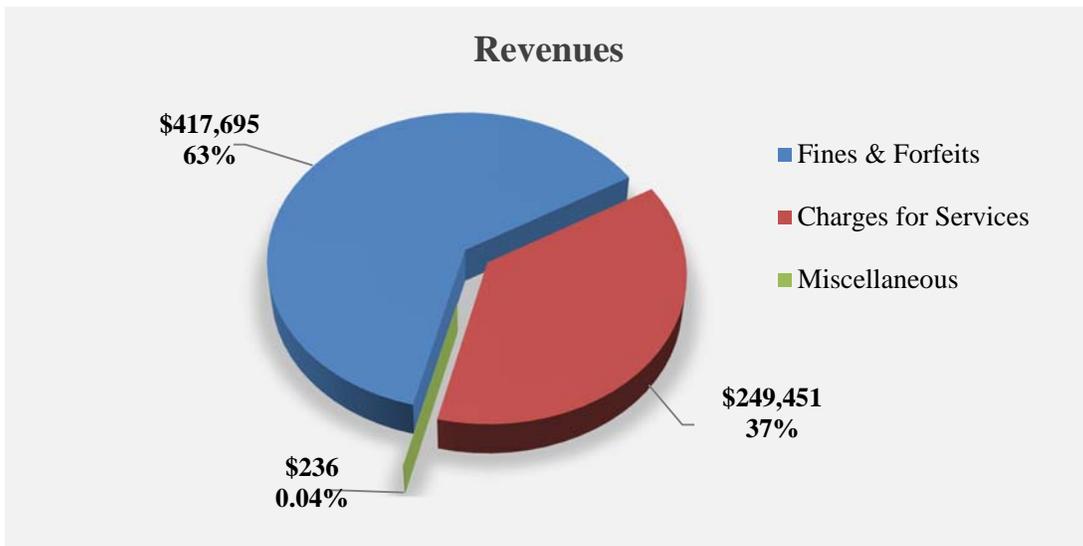
TRAVIS COUNTY
JUSTICE OF THE PEACE
PRECINCT 4



As of April 2016

FISCAL YEAR 2016 FINANCIAL DATA

During fiscal year 2016, the Travis County Justice of the Peace, Precinct 4 received \$417,695 in fines and forfeits revenue, \$249,451 in charges for services, and \$236 in miscellaneous revenue. Salaries and Benefits, which totaled \$1,136,321, represented approximately 98 percent of their expenditures. The details for their revenue and expenditures are provided below using pie graphs for data visualization:



BUSINESS PROCESS RISK PROFILES

MISSION AND OBJECTIVES

This office's main objective for both the civil and criminal divisions is a focus on the transition to an electronic court that will improve communication with and service to citizens, businesses, and other agencies. The court management system (Odyssey) will integrate with other databases, such as those maintained by TCSO and DPS, to improve the efficiency of handling issued citations. The system will have an ability to store court documents electronically to give the public greater access to citation court information.

Civil

The goal of the Civil Division is to process and dispose of civil cases in an efficient and timely manner, using innovative technology to improve communication and services offered to citizens, businesses, and other agencies. Trials conducted in the JP4 Civil Division include bench and jury trials for civil cases involving debt claims, small claims not to exceed \$10,000, evictions of tenants from properties by the owners, and landlord tenant disputes. This court also presides over administrative hearings such as the suspension of a driver's license, issuance of an occupational driver's license, unlawful towing, and other magisterial matters as required by law.

Criminal

The goal of the Criminal Division is to process and dispose of criminal cases in an efficient and timely manner. Trials in the JP4 Criminal Division include both bench and jury trials for fine-only criminal offenses involving traffic offenses and non-traffic Class C offenses for adults and juveniles. This court also presides over miscellaneous criminal matters such as peace bond hearings, disposition of stolen property hearings, and other magisterial matters as required by law.

Accounting

The Accounting Division provides financial resources to all of JP4's divisions. Accounting is responsible for preparing daily reconciliations of receipts and till reports for the collection of court costs, fines, and fees. This division is responsible for adjusting fees in the Odyssey Financial Manager System (OFM) for court ordered modifications, such as dismissals and reductions for community service performed.

This division is also responsible for processing disbursements for a variety of services, including refunds of overpayments, releases of bonds, and fund remittances to the County Treasurer and various government agencies. In addition, this division prepares monthly departmental financial statements and bank reconciliations.

SIGNIFICANT ACTIVITIES

Accounts Payable

Disbursements for both civil and criminal cases are processed by the Accounting Division and include refunds for overpayments, releases for bonds, fees to the County Treasurer and other government agencies, and unclaimed funds to the State and/or Treasurer. Checks for refunds and bond releases

are processed as needed, and fees to other agencies are disbursed monthly. Fees due to the Treasurer are remitted via ACH on a daily basis and Accounting initiates the entry in the SAP system for each remittance. Furthermore, unclaimed funds that are eligible to be escheated are remitted annually to the State and Treasurer as required by statute.

Cash Handling

Cash handling procedures include receiving payments in the mail, on the phone, and in person; researching unknown payments; collecting payments in the form of cash, checks, credit cards, etc.; posting payments in the system; issuing receipts; and performing the daily closeout reconciliation. The court clerks in both the Civil and Criminal Divisions are responsible for these cash handling duties.

Types of collections

Mailed-in payments are received daily, with civil and criminal collections being recorded on separate mail logs. Two employees are present and responsible for opening the mail, date stamping applicable documents, endorsing all checks and money orders, and completing the mail payment logs. Mail payments are receipted in the system by a separate employee who does not open the mail.

Online and telephone payments can only be made by credit/debit card. Telephone payments are processed using the EZNet System, which provides a reference number when the transaction is confirmed. The court clerk then posts the payment to the client's account in Odyssey, notes the reference number, and saves the receipt copy. Online payments for criminal fees are processed with Verifone, and Odyssey is automatically updated when payment is confirmed. Online payments for civil cases are processed in the E-File system, and this system works with Odyssey to automatically create the case and receipt the payment. A copy of the system-generated receipt is emailed to the customer.

Manual receipts are only issued when Odyssey is not functioning, such as during a power outage. The manual receipts have three parts: the white copy is given to the customer, the yellow copy is attached to the Odyssey receipt once it is posted in the system, and the pink copy remains in the receipt book. There is one manual receipt book for criminal collections and a separate receipt book for civil collections. Both receipt books are stored in a drawer at the front window.

Daily closeout

Court clerks are responsible for closing their till at the end of each day and ensuring their total collections agree to the applicable Odyssey report. The locked till bags and applicable reports are then reviewed and verified by a Court Clerk II.

The Court Services Court Administrator performs a daily reconciliation, which includes reconciling all collections using an Odyssey deposit analysis report, E-File report, Verifone report, EZNet report, and a bond report. Once all items are verified and agreed to the applicable reports, deposit slips are prepared, and the cash, checks, and money orders are placed in the deposit bags for pickup by the armored car service. Finally, the deposit is closed in Odyssey and exported to the Accounting Division.

The Accounting Division reviews the daily deposit report and supporting documentation to verify the deposit totals agree to the amounts deposited in the bank, including the credit card funds received from the processing entity. Once the deposits are verified, the deposit batches for each court clerk are

posted in Odyssey, which automatically exports the batches to the Odyssey Financial Manager (OFM).

Court Functions

JP4 court functions include bonds and interpreting services.

Bonds

Both civil and criminal bonds such as cash, surety, and custodial bonds can be posted at the JP4 Office. Civil bonds are posted pending appeals or as a promise to pay for court-ordered damages, while criminal bonds are posted as a sworn agreement by the defendant that he/she will return to court as ordered. The court clerks are responsible for collecting, posting, and receipting these bonds in Odyssey. The Accounting Division is responsible for managing and disbursing the civil and criminal bonds when ordered to by the judge.

Interpreting services

Parties to a case are encouraged to bring their own interpreter whenever possible. However, the court will provide this service as needed. At times, the court is able to utilize a member of its staff (e.g., Spanish to English). For other languages, an interpreting service called Language Line is utilized. If a party needs a sign language interpreter, the Travis County sign language interpreter is provided.

Facilities

The JP4 Office is located on McKinney Falls Parkway with the Constable, Precinct 4 Office. The Constable, Precinct 4 Office is responsible for providing appropriate protection for court staff and facilities, the general public, and the judicial process as a whole. They are to provide for immediate annunciation of emergency situations and to assist in incident-prevention efforts.

For FY17, the Facilities Management Department Security Division has initiated a three year county-wide security assessment for all County locations. This assessment will provide an emergency response and action plan for operational and physical security, as well as a Security Training Coordinator to train staff on proper emergency procedures/protocols.

Fixed Assets

All office holders and department heads are required to adhere to the Travis County Purchasing & Asset Policy and Procedures adopted by the Commissioners Court. Specifically, Ch. 32.351 “User Department Responsibilities” details the requirements for purchasing, renting/leasing, transferring, disposing, and retiring fixed assets. It also requires that an annual physical inventory of all assets assigned to the applicable office be performed. This helps ensure an accurate fixed asset listing, safeguards office fixed assets, and provides accountability.

General Ledger

On a monthly basis, the Accounting Division reconciles the QuickBooks general ledger accounts to supporting records and posts necessary journal entries to QuickBooks. 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), as well as facilitate the correction of any discrepancies. Also, month-end bank reconciliations are performed in order to verify that the weekly reconciliations are accurate, that any discrepancies have been timely corrected, and to prepare the financial statements.

Inventory

The JP4 Office maintains minimal inventory including typical office supplies (e.g., Post-it notes, staples, pens). Items are ordered on an as-needed basis and are processed via shopping cart in the Travis County Financial System, SAP.

IT and Information Systems

The Travis County Justice of the Peace Offices have implemented a court management system, Odyssey, to track and document case records and their associated court costs, fines, and fees. Odyssey allows court documents to be scanned and stored electronically, which will give the public easier access to citation court information. The system will integrate with various law enforcement information systems to provide more accurate and complete information in a timely manner.

Reporting

The Accounting Division reviews system-generated reports from Odyssey, which support the financial statements, to identify errors that need to be corrected, accruals and prepayments that need to be made, and trends that need to be highlighted. When complete, the financial statements are approved and provided to the County Auditor's Office.

Revenue Generation

The Revenue Generation process at the JP4 Office includes assessing, entering, and adjusting court costs, fines, and fees. This function also includes preparing and maintaining the supporting documentation for case files, as well as securing confidential/sensitive information.

All civil and criminal court costs, fines, and fees are assessed by the court clerks. The civil court clerks receive the civil petition, verify all necessary forms are properly completed and signed, and enter the case information in Odyssey. Odyssey automatically assigns a case number and calculates the court costs and fees based on the case information.

Various ticketing agencies submit citations that were issued within JP4's jurisdiction. The criminal court clerks receive these citations via interoffice mail, drop-off, or electronically from two websites. The first website is Brazos (my.brazostech.com), which is used by the Travis County Sheriff's Office. The second website is Parking Mobility (parkingmobility.com), which is used by volunteers issuing citations for handicap parking violations. The citations and supporting documents are scanned and attached to the case file in Odyssey.

Adjustments made in Odyssey to the court costs, fines, or fees owed on a party's account include: applying a bond release, a reduction for community service performed, a credit for jail time served, waiving fees when the charges are dismissed, and NSF/chargebacks. All adjustments are supported by applicable documents that are scanned and uploaded to the party's case in the system. Changes in court costs, fines, and fees that occur via statute, Commissioners Court, OCA, or AG Opinion are tracked by the Financial Manager and updated in Odyssey by the Business Analyst.

BUSINESS PROCESS RISKS AND RISK RATINGS

The following table depicts the risk ratings for the JP4 Office's business areas:

Business Process	Risk Rating
Accounts Payable	Low
Cash Handling	Medium
Court Functions	Low
Facilities	Medium
Fixed Assets	Low
General Ledger	Low
Inventory	Low
IT & Informational Services	Medium
Reporting	Low
Revenue Generation	Low

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

1. Collections (i.e. cash, credit cards, etc.) should be properly tracked, reviewed, and accounted for to prevent loss or misappropriation.
2. Implementation and maintenance of sufficient cash handling and bank reconciliation controls should occur to safeguard funds from loss or misappropriation.
3. To prevent a variety of legal, fiduciary, and financial losses, County data must be secured from theft/unauthorized access.
4. Changes to a user's system access, including granting additional privileges, should be properly managed to help ensure a user is not granted unauthorized access to system functions and County data is kept secure.
5. In order to help ensure that proper supporting documentation is maintained and that court cases proceed properly, case information should be properly recorded and tracked.
6. Sensitive information should be properly secured from unauthorized parties to prevent the loss or misuse of that data.
7. Implement an Emergency Action and Recovery Plan to address security breaches, interruptions to daily operations resulting from catastrophic events, and concerns of employee safety.

AREAS OF CONCERN

CASH HANDLING

Manual Receipts

When multiple-copy manual receipts are properly used, an audit trail for the cash receipts is created that can be used to verify all amounts collected are deposited. In contrast, when a manual receipt book is stolen and used to misappropriate cash receipts, there is no record of the transaction, making it possible to misappropriate funds without detection. For this reason, it is important to control access to manual receipt books.

The manual receipt book utilized by the JP4 Office is stored at the front desk, rather than in a locked area or safe. Also, this receipt book is used by a number of employees, instead of each employee being assigned an individual receipt book. When a manual receipt is issued, it does not appear that a verification is performed to ensure that the funds related to the receipt were deposited. Finally, it appears that the manual receipt book is not periodically examined to ensure that there are no missing receipts.

IT & INFORMATION SYSTEMS

Information Security

Information technology security, when implemented appropriately, can be valuable to an organization by protecting its financial and physical resources, employees, reputation, and other tangible and intangible assets. Information systems general controls are the structures, policies, and procedures that apply to an organization's overall computer operations. Government information systems may be used to store and process sensitive or confidential data including court proceedings (civil and criminal) as well as law enforcement and judicial operations.

Our understanding of general controls was obtained through interviews with management and the security administrator, reviewing the applications' documentation, and observing the physical location of each office. When we were documenting the information system processes, we noted the following:

1. The office does not have a written information security policy. While information security policies and procedures are in place, there has been no formal distribution or introduction of these policies across the office. Security policies and procedures form the foundation of how information security is implemented, performed, and enforced throughout the organization. Without a defined set of policies, JP4 employees may not be aware of appropriate security procedures, which could lead to a breakdown in controls over time.
2. Gaps exist within access control-related processes which may lead to the overall weakening of the network environment. For example, access request procedures for modifying an employee's system access upon a change in roles do not exist. The current system allows office managers to request system access for a new employee to mirror an existing employee's access role within the office. The access control process does not include a formal review for the level of access being granted before the additional privileges are assigned. Over time, this may grant excessive access to employees, which may result in unauthorized access to system functions and data.

3. Formalized business continuity planning and testing has not been defined at the JP4 Office. This includes an updated business impact analysis, IT disaster recovery plan, and a business resumption plan. While unofficial preparedness procedures are in place, these procedures do not cover all types of continuity issues and may not be sufficient in the event of a localized disaster such as a fire or flood in the area. Without defined response procedures, JP4 may suffer prolonged downtime due to an operational interruption or may not be able to fully recover operations in a timely manner.

FACILITIES

Court Security

Currently, the JP4 Office does not have an incident or emergency response plan in place. The Auditor's office understands the difficult challenge of balancing access to the court and maintaining a secure environment where all parties are safe to conduct business. Thus, the Auditor's office recommends that the department develop policies and procedures to enhance courtroom security awareness by reviewing security measures and increasing specialized incident employee training.

Each court is different due to its location and size and the community in which it resides. Therefore, there is no one solution to issues concerning court security. Because of this, each court must collaborate with law enforcement, emergency agencies, facilities management, and other entities to properly plan and develop incident and emergency response plans to ensure the safety of all stakeholders, while maintaining accessibility to this court.

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. 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 to train office staff. JP4 should initiate an interim security plan until the FMD Security Division is able to evaluate this site and assist with implementation of a complete emergency response plan.