

Travis County Justice of the Peace, Precinct 5

2016 Inherent Risk Assessment

TRAVIS COUNTY AUDITOR'S OFFICE
Risk Evaluation & Consulting Division

March 1, 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 Herb Evans
Justice of the Peace, Precinct 5

From: Nicki Riley, CPA
Travis County Auditor

Date: March 1, 2017

Re: 2016 Risk Assessment – Justice of the Peace, Precinct 5

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 5 (JP5) Office. The objective of the risk assessment was to assist JP5 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 JP5'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 the report. The organizational structure, financial data, mission and objectives, and significant activities for JP5 are provided on pages 9 through 14. The details of each division's risk assessment, including the identified business processes, inherent risks, controls implemented by management, and the inherent risk ratings, are provided on pages 15 through 19.

BACKGROUND

Justices of the peace handle both civil and criminal cases, including small claims court, justice court, and administrative hearings. In practical terms, these are lawsuits over debts, evictions, car accidents, unlawful towing, and property.

Their criminal workload involves disposing of all Class C criminal misdemeanor complaints, such as traffic citations, issuances of bad checks, and others. These cases involve assessing and collecting payments, setting contested cases for trial, and pretrial hearings with the county prosecutor.

Other duties include presiding over peace bond hearings, reviewing applications for mental health or chemically dependent commitments, conducting compulsory school attendance trials, and giving warnings required by law to juveniles. They issue warrants for, and conduct hearings concerning, seizure and disposition of cruelly treated animals. Most JPs perform marriage ceremonies as well.

SCOPE

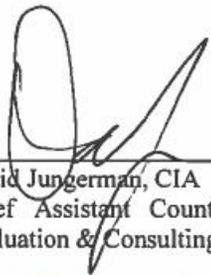
The risk assessment covered the operations of JP5 and was limited to the business processes that were in place during the time the risk assessment was being performed - the three months ending September 30, 2016. In addition, only the inherent risks were rated, meaning there were no tests of controls or transactions to assess control risk. All client meetings were held at the JP5 Office.

ENGAGEMENT TEAM

Lisa Denton, CFE, Senior Auditor
Camille Cortez, Staff Auditor
Jennifer Bodiker, Staff Auditor
John Gomez, Staff Auditor

CLOSING

This report is intended solely for the information and use of the JP5 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
Angelica Torres, Court Administrator, Justice of the Peace, Pct. 5
Joe Alvarado, Financial Manager, Justice of the Peace, Pct. 5
Frank Stover, Atchley and Associates, CPA's
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, 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.

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 5 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	17
Accounts Payable.....	17
Cash Handling	17
Fixed Assets	18
IT & Information Systems	18
Revenue Generation	19

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 JP5 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

We rated the risks inherent to the business processes handled by all of JP5 on a five-level scale from very low to very high. A summary of the risk ratings is presented in graph form on page 6 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 JP5, 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 three business processes in terms of inherent risk are provided below:

<u>Business Process</u>	<u>Risk Rating</u>
Accounts Payable	Medium
Cash Handling	Medium
Revenue Generation	Medium

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

DETAILED REPORT

RISK ASSESSMENT PROCESS

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

DATA GATHERING

In order to perform an accurate and thorough risk assessment, the first step is becoming familiar with the nature of the entity's business activities. To begin this process, we requested the following documents from JP5:

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 5 web page (<https://www.traviscountytexas.gov/justices-of-peace/jp5>)

Before meeting with the JP5 employees, we reviewed the above documentation, prior audit reports, Texas statutes pertaining to the responsibilities of JP5, 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 Court Administrator, Accounting Manager, Associate Accountant, and Business Analyst at their office located in the Travis County Courthouse. At this meeting we provided an explanation of how our office performs risk assessments, as well as the anticipated timeline.

We later held meetings with the Court Administrator, Court Services Management Admin Coordinator, and Accounting Manager, 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 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 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 JP5 include the following:

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

POTENTIAL RISKS

To identify the potential risks that could prevent JP5 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 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 JP5's staff and management are very dedicated to improving all aspects of their processes, providing excellent customer service, and maintaining the superior reputation of the office.

RATE INHERENT RISKS

PROCESS RISK RATING

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

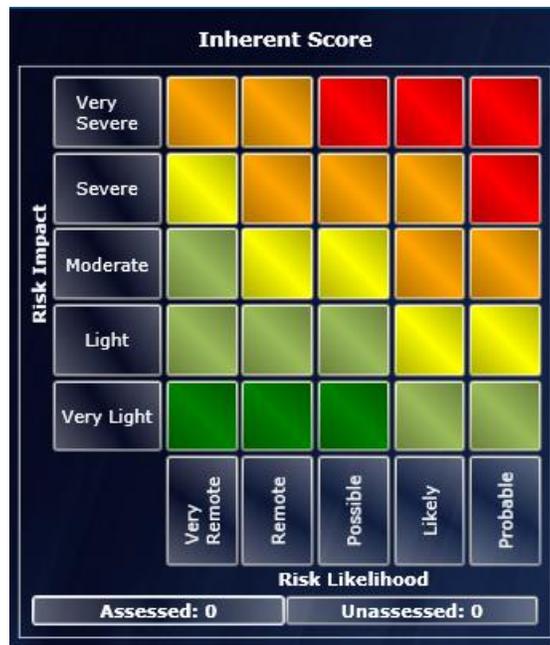
IMPACT

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

LIKELIHOOD

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

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



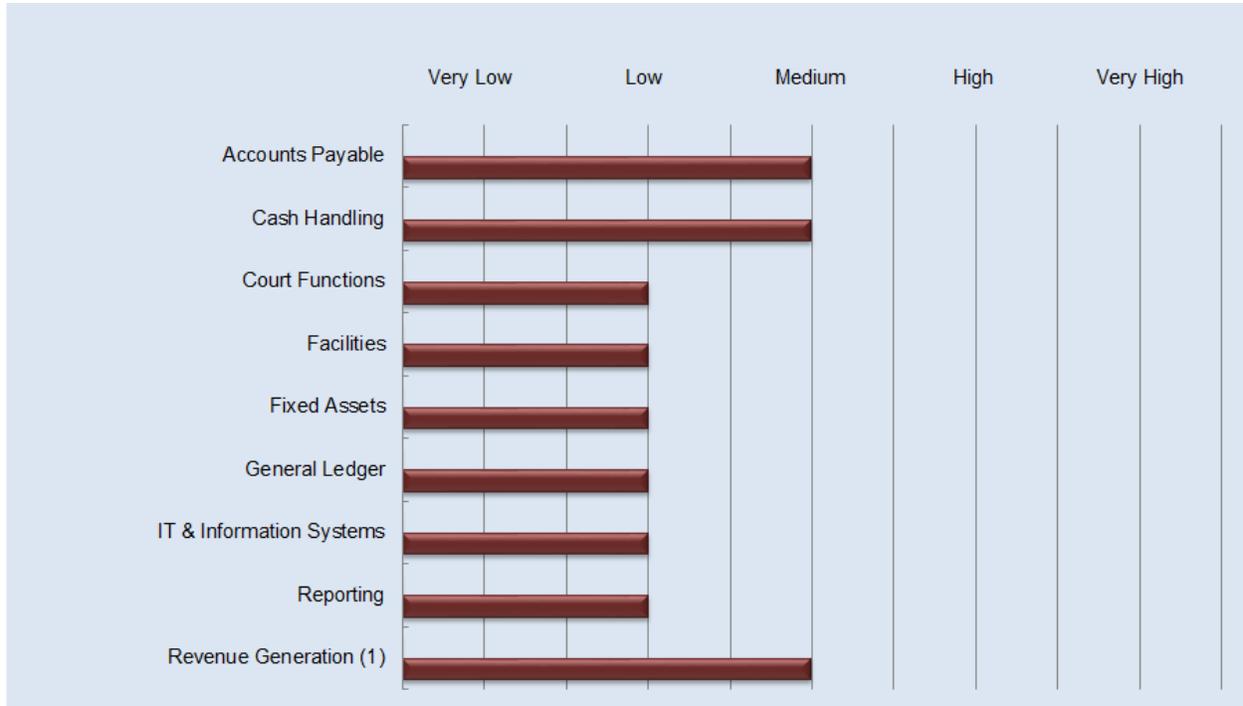
Using this matrix, the inherent risk for each business process was rated on a five-level scale as follows:

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

SUMMARY OF RESULTS

GRAPH 1 – RISK PROFILE BY BUSINESS PROCESS

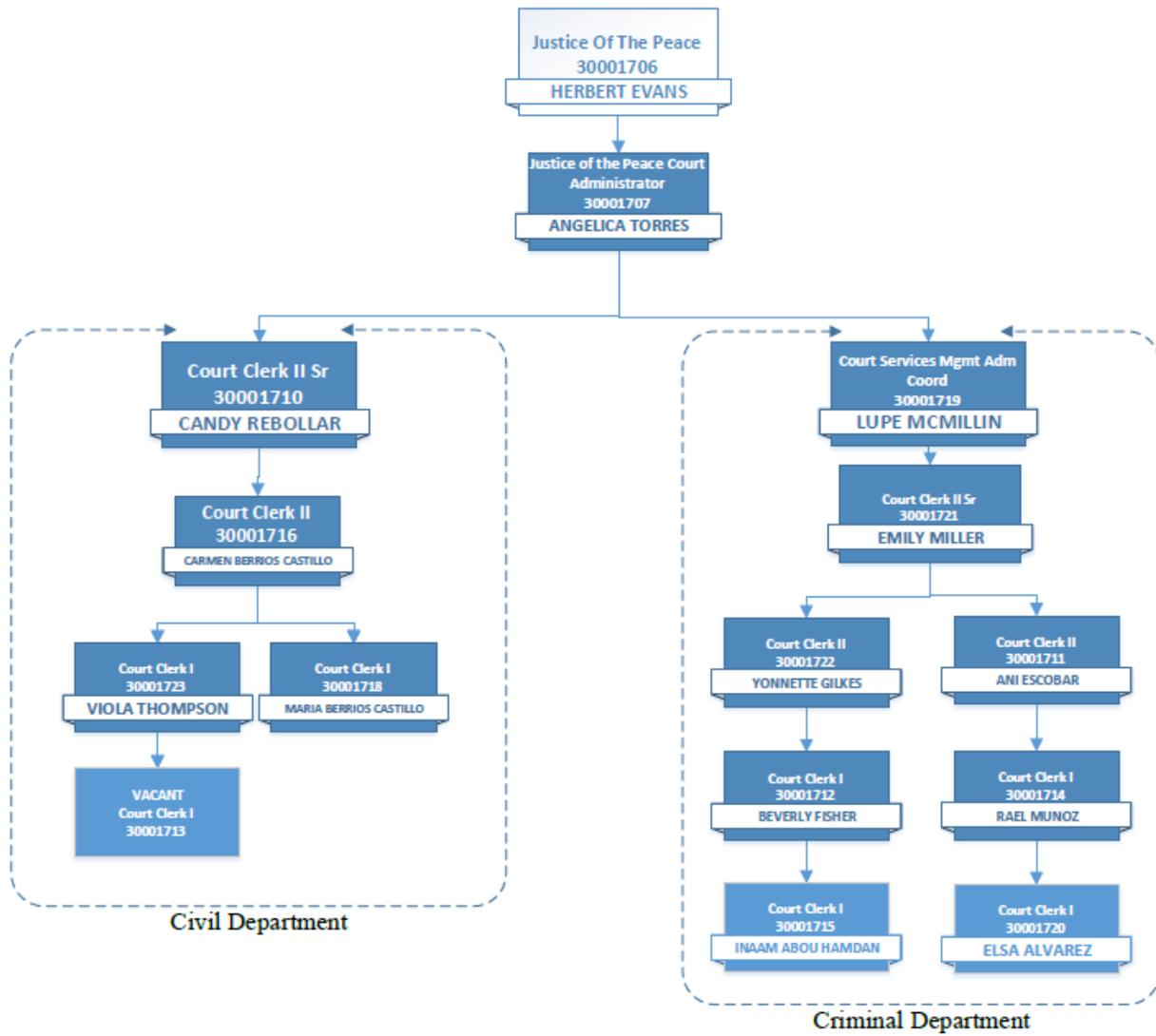
To provide visibility into the business processes which pose the greatest risk to JP5, we present the results in graph form below:



Although most of the business processes included in the above graph are self-explanatory, we have included the following additional information:

(1) Revenue Generation – Although there are many activities that fall under the Revenue Generation process, the ones that are applicable to the JP5 Office include 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.

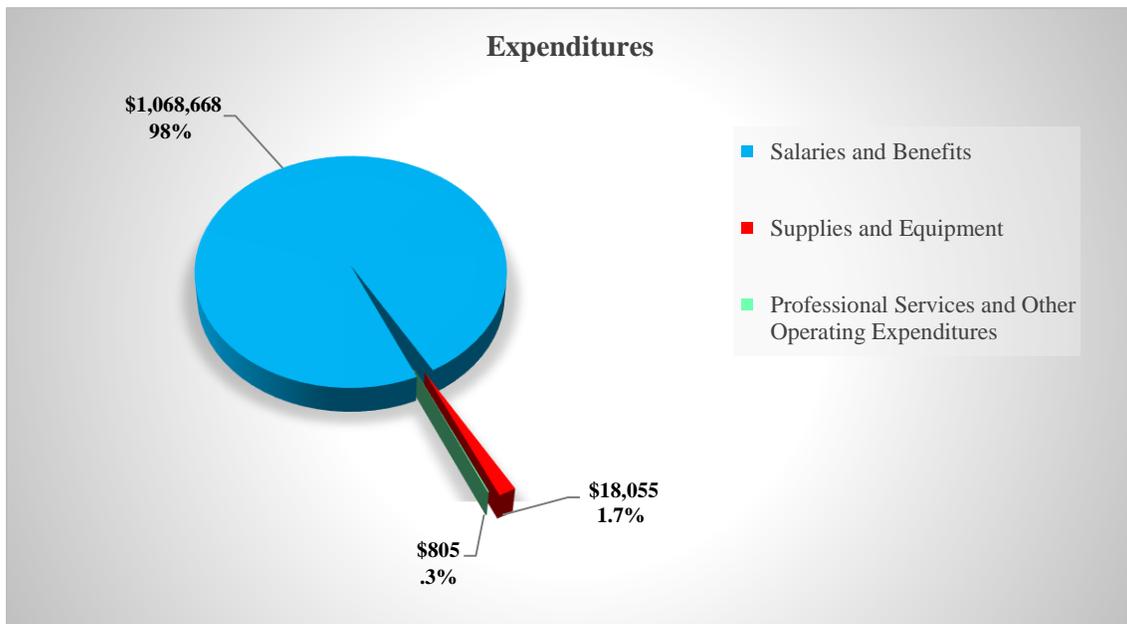
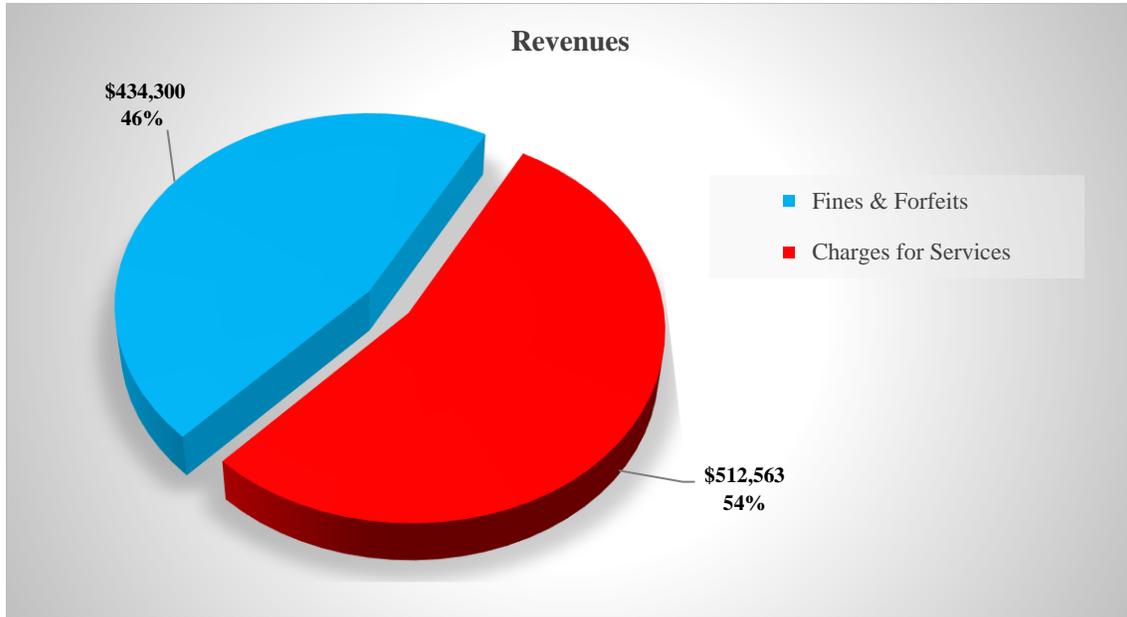
JUSTICE OF THE PEACE PRECINCT 5 ORGANIZATIONAL CHART



As of March 2016

FISCAL YEAR 2016 FINANCIAL DATA

During fiscal year 2016, the Travis County Justice of the Peace, Precinct 5 received \$434,300 in fines and forfeits revenue and \$512,563 in charges for services. Salaries and Benefits represented approximately 98 percent of their expenditures, which totaled \$1,068,668. The details for their revenue and expenditures are provided below in graph form.



BUSINESS PROCESS RISK PROFILES

MISSION AND OBJECTIVES

Civil

The goal of the Civil Division is to process and dispose of civil cases in an efficient and timely manner. Trials conducted in the JP5 Civil Division include both 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 JP5 Criminal Division include both bench and jury trials for fine-only criminal offenses involving traffic offenses, non-traffic Class C offenses, and minor juvenile offenses. 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 JP5'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 agencies (e.g., State Comptroller, Texas DPS, etc.). 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 Court Administrator and Accounting Division. These disbursements include refunds for overpayments, releases for bonds, fees to the County Treasurer and other agencies (e.g., State Comptroller, Texas DPS, and APD), 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 once each month. 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. Finally, 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, online, by 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. A civil clerk is responsible for opening the mail and date stamping applicable documents. The civil and criminal mail items are separated, with the civil items going to a second civil clerk and the criminal items to a criminal clerk. These employees complete the mail payment logs, receipt the payments in Odyssey, and endorse all checks and money orders.

When in-person payments are made with cash, check, or money order, the court clerk inquires in the Odyssey system to locate the applicable case information. The relevant case number is selected and a receipt is generated. The payment fields, including payor name, payment type, check/money order number, and amount paid, are then entered. The amount of the payment is automatically allocated to the outstanding fees. The check/money order is endorsed, if applicable, and placed in a locked till bag along with any cash received. Finally, the customer receives a printed receipt.

Online and telephone payments may 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 in Odyssey. Online payments for criminal fees are processed with Verifone and Odyssey is automatically updated when the payment is confirmed. Online payments for civil cases are processed in the E-File system, and this system works with Odyssey to automatically create both the case and 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 are in 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. Each court clerk has a manual receipt book that is kept in their locked till bag.

Daily closeout

Each court clerk is 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 the Court Administrator.

Daily reconciliation

The Court Administrator performs a daily reconciliation, which includes reconciling all collections using an Odyssey deposit analysis report, E-File report, credit cards report, and a bond report. Once all items are verified and agreed to the applicable report, 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 that 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

Bonds

Both civil and criminal bonds such as cash, surety, and custodial bonds can be posted at the JP5 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 Court Administrator and Accounting Division are 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 JP5 Office is located in the Travis County Heman Marion Sweatt Courthouse. The Sheriff's 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 campus-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, helping to ensure an accurate fixed asset listing, safeguarding office fixed assets, and providing accountability and accounting accuracy. The Court Administrator tracks the fixed assets for the JP5 Office.

General Ledger

On a monthly basis, the Accounting Division reconciles the general ledger accounts to supporting records and posts necessary journal entries. 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.

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, while E-filing allows parties to file petitions online and the Travis County JP5 website allows parties to make online payments with credit cards.

Reporting

The Accounting Division reviews system generated reports, which support the financial statements, to identify errors for correction, necessary accruals and prepayments, and trends that should 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 JP5 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 JP5's jurisdiction. The criminal court clerks receive these citations via drop-off and interoffice mail. The citations are entered into Odyssey, and the supporting documents are scanned and attached to the case in Odyssey. Finally, the original documents for both civil and criminal cases are placed in a case file and stored in the JP5 office.

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, and the originals are placed in the case file. All court clerks, managers, and accounting staff have access to make adjustments in Odyssey.

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 Project Manager.

BUSINESS PROCESS RISKS AND RISK RATINGS

The following chart depicts the risk ratings for the JP5 Office's business areas:

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

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

1. Disbursements should be properly prepared, accounted for, and approved to help prevent misappropriation or incorrect distributions of funds.
2. Collections (i.e. cash, credit cards, etc.) should be properly tracked, reviewed, and accounted for to prevent loss or misappropriation.
3. Implementation and maintenance of sufficient cash handling and bank reconciliation controls should occur to safeguard funds from loss or misappropriation.
4. Fixed assets should be tagged, tracked, and safeguarded thereby ensuring accountability and accounting accuracy.
5. Inventory and supplies should be inspected, tracked, and protected by secure access points to prevent the loss or theft of these items.
6. To prevent a variety of legal, fiduciary and financial losses, County data should be secured from theft/unauthorized access.
7. 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.
8. Managerial review of adjustments to fees should occur to ensure collections are not lost or misappropriated due to unauthorized adjustments in the system.

9. 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.
10. Sensitive information should be properly secured from unauthorized parties to prevent the loss or misuse of that data.

AREAS OF CONCERN

ACCOUNTS PAYABLE

Incompatible Duties and Internal Controls

It is important to have strong internal controls in place for the disbursement of funds to reduce the risk of loss or theft of County assets. This includes ensuring that employees are not able to perform “incompatible duties” which could allow them to both misappropriate County assets and to conceal this act. When we documented the accounts payable and disbursement processes for JP5, we noted the following incompatible duties and other internal controls that were not in place:

1. The Court Administrator has access to make fee adjustments, including full dismissal of charges, and also issues checks for overpayments, refunds, and bond releases. For criminal cases, checks are often issued to the original payor, who is not necessarily the defendant.
2. The Court Administrator signs and mails the checks. Detailed supporting documentation is not provided to an independent reviewer; therefore, a managerial review and documented authorization of disbursements is not being performed.
3. All checks are kept in a locked cabinet in the Court Administrator’s office, the office of the employee preparing and signing the checks.

CASH HANDLING

Manual Receipts

When multiple-copy manual receipts are properly utilized, an audit trail for the cash receipts is created that can be used to verify all amounts collected are deposited and posted to the system. 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 secure and reconcile manual receipts to ensure they are tracked and accounted for.

When a manual receipt is issued by the JP5 Office, it does not appear that a reconciliation is performed to ensure all receipts are posted and cross referenced in the system and that there are no missing receipts. Also, when a manual receipt is voided, it is voided in the system, but it is not voided and defaced in the receipt book.

Incompatible Duties

It is important to have strong internal controls in place in order to reduce the risk of loss or theft of County assets, including funds on hand. This includes ensuring that employees are not able to perform “incompatible duties” which could allow them to both misappropriate County assets and to conceal this act. When we documented the cash handling processes for JP5, we noted that the Court Administrator has access to receipt payments, void receipts, and adjust fees, including full dismissal of charges. This employee is also responsible for reviewing and reconciling the clerks’ tills and preparing the bank deposit.

Mail Log

Another method of misappropriating funds without detection is the theft of funds received in the mail. The risk of this occurring can be mitigated by implementing a policy requiring that two employees are present when the incoming mail is opened. Also, the employee who opens the mail should not have access to the receipting software. Finally, an independent review of the mail log to verify that all mail payments are deposited helps ensure that these funds are properly handled.

At the JP5 Office, only one civil court clerk opens the mail, and this employee also has access to receipt funds in the system, as well as adjusting fees. We also noted that checks received in the mail are not stamped with a restrictive endorsement until they have been posted.

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 to help ensure an accurate fixed asset listing and safeguard office fixed assets, providing accountability and accounting accuracy.

At the time of the risk assessment, we noted the Court Administrator for the JP5 Office began tracking and performing inventories for the fixed assets approximately six months earlier. Fixed assets had not previously been tracked or inventoried.

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) and law enforcement and judicial operations.

The auditor’s understanding of general controls was obtained through interviews with management and the security administrator, reviewing applications’ documentation, and observing the physical location of each office. When we documented 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 the 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, JP5 employees may not be aware of appropriate security procedures, which could lead to a breakdown of 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 have not been defined at the JP5 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, JP5 may suffer prolonged downtime due to an operational interruption or may not be able to fully recover operations in a timely manner.

REVENUE GENERATION

Incompatible Duties

Proper segregation of duties between case creation in Odyssey, assessing fees, adjusting fees, and receipting payments is critical to limit the means to misappropriate funds and conceal the theft. For instance, an employee could conceal the theft of funds by adjusting/reducing unpaid fees, collecting the original, higher payment, receipting the lower amount, and misappropriating the difference.

During the risk assessment, we noted that all court clerks have the ability to receipt collections and make adjustments to fees, fines, and court costs in the Odyssey system. Procedurally, all adjustments should be supported by scanned documents uploaded into the system and maintained in the case file; however, there is no supervisory review of these adjustments, which we recommend.