
JEMEZ MOUNTAINS ELECTRIC COOPERATIVE, INC.

INTERNAL CONTROL PROCESS CONSULTATION REPORT

August 18, 2022



Dawson Forensic Group

Lubbock, Texas

JEMEZ MOUNTAINS ELECTRIC COOPERATIVE, INC.

Internal Control Process Consultation Report

August 18, 2022

INDEX

Description	Bates Reference DFG00...
<u>Executive Summary</u>	<u>3 - 38</u>
Overview	3 - 4
Scope and Objectives	5 - 6
Elements of Effective Internal Control / Anti-Fraud Program Design	7 - 8
Method of Presentation	9
<u>Assessment Sections:</u>	
Section A: New Building Construction Process and Accounting	10 - 12
Section B: Capital Credits Accounting and Processing	13
Section C: Credit Card Usage and Accounting Process	14 - 15
Section D: Policies / Bylaws Review	16 - 19
Section E: Additions to Scope	20 - 27
Section F: Fraud Risk Assessment	28
Section G: Documentation of Internal Controls / Anti-Fraud Program	29 - 33
Section H: Communication: Anti-Fraud Program / Fraud Awareness Training	34 - 35
Section I: Monitoring and Routine Maintenance	36 - 37
Completion Issues	38
<u>Exhibits</u>	
Exhibit D1 Sample Code of Ethics	39 - 42
Exhibit D2 Sample Fraud / Fraud Reporting Policy	43 - 46
Exhibit D3 Presumption of Privacy Policy Example Provisions	47 - 48
Exhibit D4 Anti-Bribery / Anti-Corruption Policy	49 - 54
Exhibit E1 New Vendor Establishment Form	55 - 56
Exhibit E2 Existing Vendor Information Change Form	57 - 58
Exhibit E3 Sample Conflict of Interest Form	59 - 60
Exhibit E4 Benford's Law - Presentation/Training Extract	61 - 101
Exhibit F1 Fraud Risk Assessment Tool	102 - 137
Exhibit F2 Fraud Risk Assessment Framework	138 - 139
Exhibit G1 Sample Control Activities Documentation Form	140 - 141
Exhibit H1 Establishing an Effective Anti-Fraud Training Program	142 - 145
Exhibit I1 Sample Compliance Audit Program	146 - 147
Exhibit I2 Sample Compliance Audit Workpaper	148 - 149
Exhibit I3 Sample Anti-Fraud Report	150 - 151

JEMEZ MOUNTAINS ELECTRIC COOPERATIVE, INC.

INTERNAL CONTROL PROCESS CONSULTATION Executive Summary

OVERVIEW

This engagement is designed to apply to Jemez Mountains Electric Cooperative, Inc. ("JMEC", the "Cooperative"), headquartered at the Española office located in Hernandez, New Mexico. JMEC is a member-owned electric cooperative that provides power services to its designated service area.

JMEC has offices in the New Mexico cities of Española, Jemez Springs, and Cuba.

Scope: Forensic Investigation

This engagement was based on the desire of the Board of Trustees and Audit Committee to perform a forensic investigation of certain areas of concern predicated upon past and current history and knowledge of Cooperative operations. Additionally, the Audit Committee sought and included input from the membership regarding concerns that may need to be investigated or reviewed.

Before a forensic investigation can begin, there must be predication (probable cause) to conduct the investigation. This predication is exhibited by the existence of information or documentation that at least indicates that a fraud may have been committed. In the absence of that type of information or documentation, we cannot legally perform a forensic investigation.

Often, a forensic investigation results in the identification of a presentable case of fraud to a trier of fact for the rendering of a verdict. *Internal Fraud* can be defined as fraud (misappropriation, theft, embezzlement, corruption, financial misstatement) that is perpetrated against an organization by its own people either individually or in collusion with others, including other outside parties such as suppliers/vendors. Accordingly, the focus is not related to any form of external attack such as cyber-security attacks or other types of theft solely perpetrated by actors external to the organization.

Scope: Internal Control Process Analysis

As the scope of the forensic investigation issues was being developed, it became apparent that there were several areas of concern that should be investigated, but that did not exhibit the necessary predication to legally investigate. As such, it was determined that these areas would be subjected to an internal control process analysis. In this type of engagement, the internal controls over the financial transaction processing and reporting areas are reviewed for effectiveness and efficiency. We then develop recommendations for controls and processes that we believe serve to strengthen the overall soundness of the financial transaction and reporting processes.

If, during the course of this analysis, issues of predication are identified, we would then be able to perform a forensic investigation into these issues.

JEMEZ MOUNTAINS ELECTRIC COOPERATIVE, INC.

INTERNAL CONTROL PROCESS CONSULTATION Executive Summary

OVERVIEW

As such, this Report presents the results of the internal control process consultation. The results of the forensic investigation are presented in a separate forensic investigation report.

This engagement was performed in accordance with Statement on Standards for Forensic Services No. 1 issued by the American Institute of Certified Public Accountants, the Code of Ethics of the Association of Certified Fraud Examiners, and in accordance with lawful forensic techniques which include, but are not limited to, examination of books and records; voluntary interviews of appropriate personnel; and other such evidence-gathering procedures as considered necessary under the circumstances.

In performing this engagement, we represent that we have no prior personal or business relationships with employees, members of the Board of Trustees, members of the Audit Committee, Mr. Michael Hastings, or members of the Cooperative.

JEMEZ MOUNTAINS ELECTRIC COOPERATIVE, INC.

INTERNAL CONTROL PROCESS CONSULTATION Executive Summary

SCOPE AND OBJECTIVES

Ultimately, the Scope of the forensic services was defined as follows:

Internal Control / Process Analysis - Scope							
1	New Building Construction Process and Accounting						
2	Capital Credit Allocations / Retirements / Overall Accounting						
3	Credit Card Usage and Accounting Process						
4	Policy / Bylaw Review						
Forensic Investigation - Scope							
1	Solar Projects: Cuba and Alcalde						
2	Former Executives - Process for Separation from Service Payments						

Internal Control Process Analysis: Goals

The overall goals are to assess/advise on current fraud-related policies, and then focus on the internal controls within specific areas of transaction processing. We seek to ensure that any “holes” in the current system are exposed and addressed.

Internal Controls Process Analysis: Objectives

The objectives of this engagement include:

- Recommendation of revisions to, or the adoption of policies that address internal fraud, including at a minimum:
 - Code of Ethics
 - Fraud Policy / Fraud Reporting Policy (Combined)
 - Removal of Employees' Presumption of Privacy Policy Provisions
 - Anti-Bribery / Anti-Corruption Policy
- Review of relevant accounting and financial reporting processes in place to gain an understanding of the status of transactional performance, recording, and reporting,

JEMEZ MOUNTAINS ELECTRIC COOPERATIVE, INC.

INTERNAL CONTROL PROCESS CONSULTATION Executive Summary

SCOPE AND OBJECTIVES

- Development of related recommendations of new performance processes that include internal controls considered necessary to enhance performance, recording, and reporting of financial transactions,
- Assistance with the implementation of any new internal control processes selected,
- Instruction to staff regarding the initial monitoring for effectiveness and efficiency of the new internal control / anti-fraud program structure – for the purpose of determining if any modifications need to be made to the newly implemented internal controls.

JEMEZ MOUNTAINS ELECTRIC COOPERATIVE, INC.

INTERNAL CONTROL PROCESS CONSULTATION Executive Summary

ELEMENTS OF EFFECTIVE INTERNAL CONTROL / ANTI-FRAUD PROGRAM DESIGN

A standard internal control process analysis includes an analysis of all six design elements of an internal control / anti-fraud program as follows:

- Anti-Fraud Environment
- Fraud Risk Assessment
- Control Activities
- Documentation of Internal Controls / Anti-Fraud Program
- Communication: Anti-Fraud Program / Fraud-Awareness Training
- Monitoring and Routine Maintenance

These elements are further described as follows:

Anti-Fraud Environment

The control environment speaks to issues of the “tone at the top”. Specifically, what is the attitude of those in control (Board of Trustees and Senior Management) regarding the importance of internal controls and the prevention of fraud? If the leadership is not concerned with the design and development of sound internal controls, then no one else will be. The control environment is evidenced by certain policies that serve as the foundation for the internal control structure / anti-fraud program. These foundational policies include an ethics policy, a fraud / fraud reporting policy, and policies that address the removal of employees’ presumptions of privacy. Recommendations in this area focus on new policy adoptions or existing policy revisions that lead to establishing a foundation for a proper anti-fraud environment.

Fraud Risk Assessment

Fraud risk assessment speaks to the issue of a constant awareness and analysis of fraud risk that may be present within Cooperative operations. Leadership should be in a constant mode of analyzing the risks associated with the performance, recording, and reporting of financial transactions. Thus, the fraud risk assessment process, as its name implies, identifies those areas of financial transaction processing and reporting with the greatest risks of fraud.

Control Activities

Control activities represent those processes and checks and balances that are implemented to address the risks of fraud identified in the fraud risk assessment. This type of engagement serves to supplement existing processes as a general rule, and to provide recommendations on new processes as needed.

Program Documentation

This element addresses how the internal control structure / anti-fraud program is documented. The program in place should be committed to written form for constant reference purposes. This also serves to provide ease of transition into different job responsibilities for employees, whether from transfers within the Cooperative or from the hiring of new employees. This insures that, over time, the performance of processes and the reasons for these processes are not lost. In the absence of written documentation, the purposes and objectives of certain processes can become diluted and somewhat invisible as the Cooperative experiences turnover.

JEMEZ MOUNTAINS ELECTRIC COOPERATIVE, INC.

INTERNAL CONTROL PROCESS CONSULTATION Executive Summary

ELEMENTS OF EFFECTIVE INTERNAL CONTROL / ANTI-FRAUD PROGRAM DESIGN

Communication: Anti-Fraud / Fraud-Awareness Training

This element includes how and when policies and internal controls are communicated to the workforce. A properly designed program is worth nothing if it is only a paper document that has not been properly communicated. Thus, the communication element is the overall Cooperative-wide anti-fraud program / fraud awareness training program.

Monitoring / Routine Maintenance

The final element of a properly functioning anti-fraud program is Monitoring. If the operation of the program is not monitored for compliance, there is no measurement by which the effectiveness of the design or operation of the program can be made. The Monitoring element also serves as the basis for the identification of any program changes that may be necessary as the nature of operations change.

These elements have been considered in the analysis of the various areas reviewed and serve as the basis for any recommendations presented in the Report.

JEMEZ MOUNTAINS ELECTRIC COOPERATIVE, INC.

INTERNAL CONTROL PROCESS CONSULTATION Executive Summary

METHOD OF PRESENTATION

Based on the Scope and stated Objectives, this Report is presented in a format that recognizes these Objectives, along with references to the six elements of an effective Anti-Fraud Program, as may apply.

Guiding Principles of Internal Control Design

The recommendations presented in this Report have been developed using several guiding principles of internal control design as follows:

Principle #1

“Always design the internal control around the position, never around the person in that position”.

The person serving in a particular position may be the most trustworthy person in the Cooperative. However, there is no real guarantee that the person will be in that position the next day. If the person in a position changes, and the internal controls were designed around that previous trustworthy person; and if the new person in that position is not trustworthy, he/she may be getting ready to reap the benefits of that position’s weak internal controls.

In developing our recommendations, we must be guided by this principle to remove any bias towards our personal positive or negative assessments about a person. As such, our recommendations are formulated regardless of “who” is serving in a particular position.

Principle #2

“The perception of detection is the strongest internal control that can ever be implemented”.

Many of the recommendations in this Report are sourced in increasing this perception. Updated policies, along with training on these policies serves to raise the overall level of fraud awareness. Additionally, periodic Cooperative-wide training that focuses on “what fraud is” can substantially raise the perception of detection since the workforce knows that Cooperative leadership takes seriously the risk of internal fraud.

Prevention Controls versus Detection Controls

Internal control recommendations included in this Report can be categorized as either Prevention controls or Detection controls. Prevention controls serve to reduce the probability that fraud will occur, while Detection controls presume that the fraud is going to occur but will be detected quickly by the detection control.

In some financial transaction processing areas, there simply are not enough employees to provide an adequate segregation of duties which is necessary for a sound internal control structure. As such, no certain prevention control will help. Thus, the detection control is designed to quickly detect those fraud transactions that cannot be prevented.

JEMEZ MOUNTAINS ELECTRIC COOPERATIVE, INC.

INTERNAL CONTROL PROCESS CONSULTATION Executive Summary

NEW BUILDING CONSTRUCTION PROCESS AND ACCOUNTING

Section A

Procedures Performed

We obtained the documentation associated with the construction of the new headquarters location. This documentation included contracts, invoices, tracking schedules, and all related information regarding this project.

We interviewed Karen Wisdom ("Wisdom"), Senior Manager of Contract Administration and Compliance as she was the lead Cooperative employee associated with this project.

Background

At the end of 2016, the request for proposals for the design architect were issued. At that time, the project was earmarked for \$7 million dollars.

Those that bid provided their bids based on what could be done for \$7 million dollars.

Through a proper bid awarding process, the bids were scored and the top two were presented to the building committee, which then presented to the Board of Trustees. Fanning, Bard & Tatum (FBT Architects, "FBT") was selected for the project. FBT was the lowest bidder for the project.

This project was not subject to Rural Utilities Service ("RUS") requirements since no RUS loans funds were to be used for the construction project.

Subsequent to this process, it was determined that the project would not be able to be completed at the \$7 million level due to existing construction industry costs. Ultimately, it was approved to be adjusted to a \$10 million project, more specifically \$10,299,009.38. This is considered a contract adjustment to the original contract rather than what is typically referred to as a change order.

In 2018, through a proper bid process, Bradbury Stamm Construction Company ("Bradbury Stamm") was selected as the general construction contractor. Bradbury Stamm was the lowest bidder of the three bids received.

Control Processes / Diligence Processes

The process was established whereby Bradbury Stamm would submit the periodic pay applications to FBT Architects to review the accuracy of the billing based on their review of the construction process that they monitored throughout the process.

The Cooperative would not pay these billings until approved as proper by FBT Architects.

Wisdom met with FBT Architects and Bradbury Stamm every Tuesday during the construction process to review progress and to ensure that the Cooperative received credit for items that were different from the original construction plans.

JEMEZ MOUNTAINS ELECTRIC COOPERATIVE, INC.

INTERNAL CONTROL PROCESS CONSULTATION Executive Summary

NEW BUILDING CONSTRUCTION PROCESS AND ACCOUNTING

Section A

Additionally, Wisdom reviewed all change orders and submitted to the Board of Trustees for approval.

Back in 2014 when Wisdom first took her current position, she established a logbook for governing body and management officials to be able to come in and review contracts, contract amendments, change orders, etc., without the risk of those contracts being unofficially released. This diligence process continues to the present time.

Project Status

As of the dates of our on-location fieldwork,

- the construction process is substantially complete but is open for issues associated with resolution on what may be done with the old headquarters building,
- A net total of \$767,490.82 has been added to the contract through change orders to arrive at the current contract sum of \$11,066,500.20,
- A total of \$10,612,650.86 had been paid against the construction contract,
- Thus, the balance to complete construction, per the contract, amounted to \$453,849.34.
- This completion amount may be subject to change based on the decision as to the future use of, or ultimate destruction of the old headquarters building.

Additional Procedures Performed

In addition to validating disbursements related to the construction and architectural contracts, we reviewed the nature and need of the amounts included as change orders and change orders credits to the construction contract.

This analysis reflects various smaller dollar amounts for items considered typical to these types of contracts such as, access control for gates, valve replacements, track lighting, etc. However, it was noted that two of the major change orders dealt with the information technology ("IT") system for the new building such as the necessary access for a communications and data connection installation, and for IT network switches. These two change orders accounted for a total of \$468,330.18 of the total of all change orders.

Other Issues

We also received information regarding allegations that the Cooperative spent \$1 million on a new board room table and over \$30,000 on the bronze dedication plaque installed in the new building's entryway foyer.

JEMEZ MOUNTAINS ELECTRIC COOPERATIVE, INC.

INTERNAL CONTROL PROCESS CONSULTATION Executive Summary

NEW BUILDING CONSTRUCTION PROCESS AND ACCOUNTING

Section A

To address these issues, we physically inspected the board room table in the new board room and noted that this is the old board table from the old headquarters building. We then reviewed disbursements for furniture and equipment for the new building noting that no board table was purchased for the new building's board room.

Regarding the bronze plaque, we obtained the invoices and payments for the casting and installation of the plaque. In total, the Cooperative paid \$12,500.

Conclusions

Typical construction contracts of this nature include the following processes:

- Concept / Idea
- Request for Proposals – Architects
- Bid Analysis
- Bid Award
- Request for Proposals – Construction General Contractor
- Bid Analysis
- Bid Award
- Review and Approval of Invoices
- Review and Approval of Disbursements
- Review and Approval of Change Orders
- Project Tracking

In each of the processes, the parties performed these functions in an exemplary manner. In fact, regarding these types of projects, the processes and documentation in support of the processes are considered to be some of the best we have encountered.

JEMEZ MOUNTAINS ELECTRIC COOPERATIVE, INC.

INTERNAL CONTROL PROCESS CONSULTATION Executive Summary

CAPITAL CREDITS ACCOUNTING AND PROCESSING

Section B

Synopsis

The allocation, retirement, accounting for, and quality of subsidiary records related to members' capital credits is paramount to the successful operation as a cooperative and the maintaining of value of membership to its members.

There have been several general ledger accounting issues in the past that have been rectified through the work of Johnny Valerio, Carmen Campbell, Geraldine Romero, and Karen Wisdom over the past several years.

The reconciliation of these general ledger accounts has involved these individuals as well as outside consultants.

These accounts affect several different accounting areas such as members' equity, amounts payable to the Foundation, and bank accounts.

Current Status

At this time, the most recent allocation of capital credits was for the 2018 year. The most recent capital credit retirement occurred in 2017.

Recommendations

Efforts should continue to prioritize the finalization of allocated capital credit subsidiary records.

Additionally, the Cooperative should adopt a goal of capital credit retirements in a pattern that will bring retirement status to a 25 to 30 year rotation.

JEMEZ MOUNTAINS ELECTRIC COOPERATIVE, INC.

INTERNAL CONTROL PROCESS CONSULTATION Executive Summary

CREDIT CARD USAGE AND ACCOUNTING PROCESS

Section C

Typically, this area in organizations is subject to the most fraud and/or abuse. We review the process of accounting for credit card use and the processes associated with obtaining support for credit card charges.

Background

Currently, there are six credit cards in use through the Wells Fargo platform; two with \$10,000 limits and four with \$5,000 limits. For travel purposes, the Cooperative utilizes per diems for meals and incidentals and does not provide cash travel advances.

In the event an employee uses their personal vehicle for business travel, they are reimbursed at the then existing IRS standard mileage rate.

As part of the month-end closing process, Geraldine Romero (Acting Chief Financial Officer), accesses the online Wells Fargo credit card activity screens and screenshots the charges. She sends these screenshots to the users and requests that all receipts be provided for all charges.

She creates a reconciliation spreadsheet that includes these charges and uses this to track when the supporting documentation (receipts) are received.

Geraldine follows up with the users to determine if there is any missing documentation.

The charges are then coded to the appropriate general ledger account.

This process is rotated periodically with Erlinda in accounting.

Once the bill payment is due, the payment on the cards is auto-drafted by Wells Fargo.

Procedures Performed

We obtained these spreadsheets that reflect this process for various months between February of 2021 through March of 2022.

We analyzed for adherence to the process noted in the background section.

We reviewed the receipts provided for charges included on the spreadsheet.

Results of Procedures Performed

We noted very few instances where the receipts had not been obtained prior to the auto-draft by Wells Fargo. This level of occurrence represents good adherence to the process. Regardless, it takes cooperation from all levels of the workforce, not just accounting, to ensure that all receipts are obtained in support of all credit card charges.

JEMEZ MOUNTAINS ELECTRIC COOPERATIVE, INC.

INTERNAL CONTROL PROCESS CONSULTATION Executive Summary

CREDIT CARD USAGE AND ACCOUNTING PROCESS

Section C

The process is considered to be well-designed, well-followed, and documented appropriately. Additionally, the rotation of this function lends to the overall strength of this process.

Recommendations

The importance of retaining receipts for all credit card usage should be recommunicated to the workforce.

Accounting staff strives for perfection in tracking these receipts. However, this can only be attained by cooperation from anyone and everyone that uses a credit card.

Particularly for business meals, the date, time, purpose, and attendees at these meals should be noted on the receipt. Additionally, it was noted that tips for meals varied from large dollar amounts to none.

As such, the Cooperative should adopt a tip guideline to ensure consistency.

JEMEZ MOUNTAINS ELECTRIC COOPERATIVE, INC.

INTERNAL CONTROL PROCESS CONSULTATION Executive Summary

POLICIES / BYLAWS REVIEW

Section D

Synopsis

As stated in the Overview, the contracting for an internal control process consultation such as this is indicative of the importance that the Board of Trustees, Audit Committee, and Management place on internal controls designed to safeguard assets. Because the Environment is a representation of the “tone-at-the-top”, this fact alone provides a certain strength in the Cooperative’s anti-fraud environment.

We reviewed existing board policies, employee policies, and Bylaws for purposes of determining additions and/or modifications which could serve to strengthen the overall anti-fraud / internal control foundation for the Cooperative.

In reviewing these items, our focus was centered on certain anti-fraud provisions that we believe to be of utmost importance.

General Comments

Regarding the Bylaws, we offer no recommendations since the content is a matter of the joint desires of the membership, the Board of Trustees, senior management, and external legal counsel. Any comments made regarding this area are made in the context of anti-fraud / internal control related items.

Currently, the existing policies include many of the provisions we look for in analyzing and assessing anti-fraud policies. The policies indicate that they have been amended periodically and may need to be consolidated in several areas as a refinement of the overall policy structure.

Additionally, within Board policies, employee policies, and the Bylaws, there are various areas that address conflicts of interest. Our comments regarding the content of these policies basically takes the position that they are adequate in design and should be diligently followed.

Recommendation

As relates to conflicts of interest, all efforts should be made to adhere to the content of policies that address these areas. For employees, full disclosure should be made of any conflicts that may exist regarding financial interests with those the Cooperative may conduct business. Additionally, for the Board of Trustees, care should be taken to recuse themselves from voting on a matter that involves a real or perceived conflict of interest.

We recommend that a Conflict of Interest Form as referenced in Section E; a sample attached to this Report as **Exhibit E3**, be completed at least annually by all employees and Board of Trustee members to enhance and encourage full disclosure which results in all parties being perceived as operating beyond reproach in conducting the business of the Cooperative.

JEMEZ MOUNTAINS ELECTRIC COOPERATIVE, INC.

INTERNAL CONTROL PROCESS CONSULTATION Executive Summary

POLICIES / BYLAWS REVIEW

Section D

Board / Employee Policies

A sound anti-fraud program environment includes a foundation made up of policies that address the overall atmosphere of the leadership in communicating the position that fraud will not be tolerated. The strength of the anti-fraud environment is evidenced by the existence and content of policies directed at anti-fraud measures. These policies and policy provisions normally should include the following:

- Code of Ethics
- Fraud / Fraud Reporting Policy (Combined)
- Removal of Employee Presumption of Privacy Provisions
- Anti-Bribery / Anti-Corruption Policy
- Prohibited Use of Heavy Equipment / Power-Operated Equipment

Specific Comments

Code of Ethics

A code of ethics is a general policy that sets out the expectations for the conduct of the workforce that communicates that fraud will not be tolerated.

More specifically, this policy addresses,

- Fair Competition,
- Conflicts of Interest,
- Gifts,
- Outside Employment,
- Confidential Information,
- How to Report Violations.

The Cooperative does have a Code of Conduct and other policies that, when considered together, includes the various components referenced here.

Attached as **Exhibit D1** is a sample Code of Ethics that may be used in the event that refinements or consolidation of existing policies is desired.

Fraud / Fraud Reporting Policy (Combined)

The Cooperative's current policies include various provisions typically included in a fraud / fraud reporting policy. However, additional provisions, and the consolidation of existing provisions into one policy, can serve to enhance the overall effectiveness of the anti-fraud environment.

JEMEZ MOUNTAINS ELECTRIC COOPERATIVE, INC.

INTERNAL CONTROL PROCESS CONSULTATION Executive Summary

POLICIES / BYLAWS REVIEW

Section D

A typical fraud / fraud reporting policy provides that fraud will not be tolerated, provides general examples of fraud, provides what will happen if fraud is suspected, provides whistleblower protection, and provides a framework for reporting suspicions of fraud.

Recommendation

Exhibit D2 to this Report provides a sample combined fraud / fraud reporting policy that the Board of Trustees should use as a guide to develop and adopt a formal policy and process. This policy should not be implemented without the review and approval of outside legal counsel.

Removal of Employee Presumption of Privacy Provisions

These provisions generally speak to the issue that the Cooperative provides the tools necessary for an employee to perform their assigned functions such as:

- Computer,
- Email,
- Internet Access,
- Phones,
- Tablets,
- Office, Desk.

As such, the Cooperative has the right to monitor and/or inspect activity within these items and an employee should have no presumption that these items are private and inaccessible.

Currently, the Cooperative addresses this removal of the presumption of privacy in Section V(M) – General Policies that addresses the use of the telephone. Without specifically stating that there is no presumption of privacy, the policy does state that the Cooperative has the right and responsibility to monitor or inspect if necessary.

Included as **Exhibit D3** to this Report is a document that includes examples of the various provisions for removal of presumptions of privacy. In the event that leadership determines to enhance various applicable policies, this information may be used as a reference.

Anti-Bribery / Anti-Corruption Policy

Due to numerous fraud cases industry-wide regarding purchasing; relationships with suppliers; awarding and administration of contracts, and collusion between organizations and outside vendors, we include this policy as a necessary foundational policy.

JEMEZ MOUNTAINS ELECTRIC COOPERATIVE, INC.

INTERNAL CONTROL PROCESS CONSULTATION Executive Summary

POLICIES / BYLAWS REVIEW

Section D

Recommendation

Exhibit D4 to this Report provides a sample Anti-Bribery / Anti-Corruption policy that the Board of Trustees should use as a guide to develop and formally adopt. This policy should not be implemented without the review and approval of outside legal counsel.

This policy applies not only to Cooperative officials and employees, but also to outside organizations that the Cooperative does or may do business with. As such, this policy should be provided to these outside organizations as applicable.

Prohibited Use of Heavy Equipment / Power-Operated Equipment

A policy of this type basically states that, “No one will be permitted to utilize for personal use or benefit, heavy / power-operated equipment, material, or facilities in possession of or owned by the Cooperative”.

Recommendation

We recommend this strict stance that no personal use of this type of equipment should be allowed.

One of the areas where we have encountered the most fraud in Cooperatives is in this very area. As an example, if employees are allowed to use a trencher owned by the Cooperative (and thus owned by the members it serves); we have seen this open the door to an entire membership that believes they should be afforded the same ability to use the equipment.

In fact, we have encountered a circumstance within the past two years where this very issue resulted in a membership upheaval that resulted in the removal of the entire Board of Directors.

Other associated issues include the wear and tear on this equipment that benefits employees, but not the membership that the equipment is supposed to serve.

Finally, we believe the liability issues associated with personal use of this type of equipment is substantial.

JEMEZ MOUNTAINS ELECTRIC COOPERATIVE, INC.

INTERNAL CONTROL PROCESS CONSULTATION Executive Summary

ADDITIONS TO SCOPE

Section E

Synopsis

As typically occurs in an engagement of this nature, we encountered several other areas related to the controls and processes for transaction processing and reporting that we determined beneficial to analyze. As such, these specific areas were added to the scope of this part of the engagement.

NEW VENDOR ESTABLISHMENT / VENDOR INFORMATION CHANGE PROCESSES

We have encountered a significant increase nationwide in shell company fraud, vendor disbursement fraud, and preferential disbursements over the past several years. The risk of this type of fraud can be mitigated through proper vendor establishment procedures, vendor information change procedures, and the use of a Conflict of Interest form.

While our Report is focused on the prevention and detection of internal fraud, the vendor disbursement process in many organizations remains an area of operation where external attacks can proliferate. We have encountered a significant increase in “social engineering” schemes, primarily the “man-in-the-middle attack”. These schemes are described as follows:

Social Engineering

“Social engineering attacks typically involve some form of psychological manipulation, fooling otherwise unsuspecting users or employees into handing over confidential or sensitive data.

Commonly, social engineering involves email or other communication that invokes urgency, fear, or similar emotions in the victim, leading the victim to promptly reveal sensitive information, click a malicious link, or open a malicious file. Because social engineering involves a human element, preventing these attacks can be tricky for enterprises”. — Nate Lord - *Social Engineering Attacks: Common Techniques and How to Prevent an Attack*, Published at DigitalGuardian.com, July 11, 2018

Man-in-the-Middle Attack

A Man-in-the-Middle (“MITM”) scheme is an attack whereby the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. Most commonly, social engineering of email communication is the method used. An example of this scheme is when the attacker, posing as the vendor, establishes communication with a Company employee. The attacker then, posing as a Company employee, establishes communication with the vendor. The attacker then requests a change in the ACH payment information (such as bank routing number and bank account number) from the valid vendor’s bank account to the attacker’s bank account.

For the Cooperative, validation-type information currently obtained for new vendors is the IRS Form W-9 – Request for Taxpayer Identification Number and Certification.

For vendor information changes, such as addresses or payment information, there is no validation process currently in place.

JEMEZ MOUNTAINS ELECTRIC COOPERATIVE, INC.

INTERNAL CONTROL PROCESS CONSULTATION Executive Summary

ADDITIONS TO SCOPE

Section E

Recommendations

To mitigate these areas of exposure, we provide the following recommendations:

A formal validation process for adding new vendors should be considered for adoption. The obtaining of a signed W-9 from the vendor is, by itself, not adequate. Additional validation procedures should be performed that include,

- Obtaining organizational documents
- Performing test emails and phone calls
- Validation of web presence – website and other social media, Google, and Google Maps
- Performing searches for duplicate address and contact information against employee database and existing vendor database
- Performing searches for duplicate bank account information against employee database and existing vendor database
- Assignment of a Vendor Information Change Code to be used for validation of future vendor-requested changes

Since Common MITM attacks focus on “changes” in vendor ACH payment information, we recommend the establishment of a formal process, including a formal form, that should be used for processing vendor-requested changes such as address and payment related information.

This process should include validation using the previously established vendor information change code, along with the completion and dual authorization of a Vendor Information Change Form.

A sample New Vendor Establishment Form **Exhibit E1**, and a sample Vendor Information Change Form **Exhibit E2**, are included as exhibits to this Report.

Additionally, for purposes of prevention of shell company fraud, we recommend that each employee and Trustee be required to complete a Conflict of Interest Form on an annual basis. This form elicits information that could identify those customers and suppliers for which the employee and/or Trustee has a financial and/or personal relationship. While fictitious shell companies would not be expected to be disclosed by a party committing shell company fraud, the requirement to complete the form increases the perception of detection substantially, which may serve to stop the committing of shell company fraud. A sample Conflict of Interest Form is included as **Exhibit E3** to this Report.

The Cooperative should conduct periodic training to raise the level of awareness of MITM attacks and the importance of adhering to proper processes to avoid being the victim of social engineering.

JEMEZ MOUNTAINS ELECTRIC COOPERATIVE, INC.

INTERNAL CONTROL PROCESS CONSULTATION Executive Summary

ADDITIONS TO SCOPE

Section E

ACH PAYMENTS TO VENDORS

Future processes will be established whereby vendors will be paid through the ACH process rather than with paper checks. Once established, the following base recommendation should be considered for implementation:

Recommendation

Once it is determined that ACH payment will be adopted for vendors, we recommend they be required to complete an ACH Authorization Form that is maintained under strict control of the Chief Financial Officer, the Controller, and the designated Accounts Payable Clerk. The ACH Authorization Form should include the same Vendor Information Change Code assigned as part of the recommendations included previously in this Report.

PURCHASE ORDER SYSTEM

Currently, there is a purchase order (PO) system in place for materials and supplies inventory, but not for non-inventory purchases. The Cooperative also has a purchase requisition form, but it generally is signed after the purchase.

Since purchasing fraud is a primary type of fraud that occurs in this industry, we believe the following recommendations should be considered for implementation:

Recommendations

Implement a PO system for all purchases, not just inventory related purchases.

Establish preapproval requirements (as evidenced by signatures) for a purchase requisition. Once approved, assign a proper PO to the purchase.

Once the item is received, require matching of the packing slip with the PO and the requisition.

Once the invoice is received, require matching of the invoice to the previously validated PO, purchase requisition, and packing slip.

STOCK INVENTORY

For purposes of this section, stock inventory refers to those items necessary for fleet maintenance such as anti-freeze, oil, filters, etc. There is an inherent difficulty in properly tracking usage of these types of items. Currently, the Cooperative has a fleet management software that is not being used. However, with the proper training and commitment, use of this software could strengthen the overall control of these items.

JEMEZ MOUNTAINS ELECTRIC COOPERATIVE, INC.

INTERNAL CONTROL PROCESS CONSULTATION Executive Summary

ADDITIONS TO SCOPE

Section E

Recommendation

Staff should experiment with the implementation of this software to determine an ultimate cost-benefit analysis of its use.

For example, if the cost to maintain the use of this software is more than the cost of large periodic adjustments due to not tracking, then acceptance of these adjustments may be the most cost-efficient scenario, and vice versa.

However, it should be noted that when unsubstantiated adjustments are allowed, it removes from the process any ability to identify theft and/or inefficiencies that may exist.

SMALL INVENTORY

Additionally, it was noted that there are times when small dollar items of inventory, such as ground rods, are purchased and coded to the Stores Clearing account. When it is time to issue to a workorder, the item is not there. This is due primarily to managing and processing transactions for three warehouses at the same time. This results in the unnecessary preparation of paperwork to create an item so that it can then be issued to a project workorder.

Recommendation

It is our understanding that staff are implementing quarterly inventory physical counts during the summer of 2022, including these types of items, in an effort to improve this processing inefficiency. We concur with this process as an attempt to improve this area of transaction processing.

As with stock inventory, the accepting of periodic adjustments as just part of the accounting process removes the ability to identify theft and/or inefficiencies that may exist.

CONTRIBUTIONS IN AID TO CONSTRUCTION

Currently, the Cooperative is behind on collection of amounts due from members under contributions in aid to construction agreements. This has been caused by the lack of assignment of a specific employee to the collecting of these amounts.

Over the past approximate twelve months, the follow-up on the more current outstanding amounts are being processed more efficiently and effectively than in the past.

JEMEZ MOUNTAINS ELECTRIC COOPERATIVE, INC.

INTERNAL CONTROL PROCESS CONSULTATION Executive Summary

ADDITIONS TO SCOPE

Section E

The amounts due to the Cooperative, by year, are as follows:

Year	Amount
2013	\$ 1,062.16
2014	5,927.89
2015	194,781.88
2016	56,218.15
2017	46,533.82
2018	27,404.30
2019	215,185.69
2020	27,270.24
2021	158,127.93
2022	12,002.14
	<u>\$ 744,514.20</u>

Recommendation

A single staff member should be assigned the responsibility for the monthly billing and collection of these amounts, including calls and letters communicating delinquency status to the applicable members. Depending on availability, the plant side of accounting (workorder) side may best be assigned this function.

In that manner, the accounting department can then review the status of uncollectible amounts and outstanding balances, and reconcile these amounts to the general ledger as part of its monthly closing functions.

In order to facilitate collection efforts, the Cooperative should implement a policy/process to determine how amounts are to be collected and/or charged-off. This process could include provisions such as,

- Notice mailed after 10 days delinquent,
- Phone call to the member after 20 days delinquent,
- Charge-off after six months delinquency with no efforts by the member to bring the balance to a current status,
- Submission of charged-off amounts to collection agency

JEMEZ MOUNTAINS ELECTRIC COOPERATIVE, INC.

INTERNAL CONTROL PROCESS CONSULTATION Executive Summary

ADDITIONS TO SCOPE

Section E

OTHER PLANT ACCOUNTING ISSUES

Currently, standard transformer installation costs and cost of removal amounts have not been updated in several years. Additionally, it was noted that there is currently a large number of open workorders.

Recommendations

There has been turnover in the workorder processing function. At this time, with some stability in that position, efforts should be continued to clean up and close as many open workorders as possible to bring this area to a more current status.

Efforts should be directed at updating standard installation costs and costs of removal. This should be prepared by someone in the plant department other than the workorder processing employee.

ACCOUNTS RECEIVABLE BILLING ADJUSTMENTS

Billing adjustments represent one of the most abused areas in cooperative operations nationwide. This type of fraud is specific to the cooperative industry since employees and board members are also typically cooperative members.

While we did not encounter this type of fraud in the Cooperative, we believe processes should be redesigned to prevent the possibility of this common type of fraud occurring. Process and control recommendations are as follows:

Recommendations

A process should be adopted that includes the prohibition of employees transacting on their own and/or family member accounts.

All member accounts receivable transactions should reflect the same process as that of members of the Cooperative such as disconnect fees, budget billing, etc.

Billing adjustments, fee reversals/removals, budget billing arrangements, payout arrangements, should be subject to the authorization of two billing related supervisors, with a final third authorization provided by the signatures of Michael Hastings or Karen Wisdom.

JEMEZ MOUNTAINS ELECTRIC COOPERATIVE, INC.

INTERNAL CONTROL PROCESS CONSULTATION Executive Summary

ADDITIONS TO SCOPE

Section E

WRITTEN PROCESS DOCUMENTATION – Overall Recommendation

As applies to all internal control processes, not just to the recommendations included in this Report, all processes (accounting, transactional, reporting) should be committed to written form. This is not a task that is completed quickly, but rather over an extended period of time.

Development of this type of information does not just include documentation such as narratives and screenshots of how to maneuver through the IT system to perform assigned functions, but more importantly includes those steps that the employee has developed instinctively over time that is part of what they do, even though it is not part of the written documentation. This is one of the primary reasons why this process takes so long.

The Cooperative has employees with many years of experience that know *how* to do their jobs, know *how best* to do their jobs, and know *why* they perform their assigned functions in the manner they perform. The loss of this type of experience and education through attrition is difficult. However, with proper written process documentation, the negative effects of attrition can be somewhat lessened.

This type of documentation serves to ensure the consistent application of job functions by employees as attrition occurs. These written processes should be designed so that the next person in a position can step into the new position with a clearer understanding of *why*, *how*, and *how best* to perform their assigned function.

ESTABLISHMENT OF INTERNAL AUDIT RELATED PROCEDURES

Currently, the Cooperative does not have an internal audit function in place. As the complexity of operations continues to grow, the performance of certain internal audit related procedures may be necessary to enhance the Monitoring and Routine Maintenance element of the anti-fraud program. These procedures focus on the previously referenced vendor establishment, disbursement, and information change processes and can be performed by existing personnel without the need to add to current staff.

Recommendations

We recommend that the Chief Financial Officer or the Controller, or a combination of both, perform the following internal audit related procedures:

Vendor Data Analytics - Master File Data

To determine if an employee may be perpetrating shell company fraud, perform an information search for duplicates between the master vendor file database and the human resources (employee) database for:

JEMEZ MOUNTAINS ELECTRIC COOPERATIVE, INC.

INTERNAL CONTROL PROCESS CONSULTATION Executive Summary

ADDITIONS TO SCOPE

Section E

1. Vendor address match to human resources database
2. Vendor bank account information match to human resources database
3. Query for vendors with no address
4. Query for vendors with missing or no contact information

To determine if the identity of a dormant/inactive vendor has been taken over:

5. Query for address changes on dormant/inactive vendors
6. Query for bank account information changes on dormant/inactive vendors
7. Query for contact information changes on dormant/inactive vendors

To determine the existence of hidden shell company vendors:

8. Search for duplicate information between vendors including Contact Information, Addresses, and Bank Account Information

Vendor Data Analytics – Transactional File Data

9. Invoice Number – Query for Sequential Patterns or Low Starting Numbers
10. Date Field:
 - Query for Invoice Dates that precede the Purchase Order Dates
 - Query for Unusual Speed of Payment Processing (invoice date compared to payment date)
11. Invoice Amount – Query for amounts below the established control threshold

Other Periodic Compliance / Audit Procedures

12. Compliance review of adherence to new vendor establishment and vendor information change processes
13. Compliance review of adherence to previously established parameters for classification as dormant/inactive vendors
14. Review of System Administrator changes to assigned employee system access
15. Performance of Benford's Law Analysis on company disbursements

Included as **Exhibit E4** to this Report is an extract from a recent training seminar we presented that introduces Benford's Law and its use for fraud detection and/or for the identification of inefficiencies in processing financial transactions. We remain available to provide additional information or training regarding Benford's Law upon request.

JEMEZ MOUNTAINS ELECTRIC COOPERATIVE, INC.

INTERNAL CONTROL PROCESS CONSULTATION Executive Summary

FRAUD RISK ASSESSMENT

Section F

As stated previously in this Report, fraud risk assessment speaks to the issue of a constant awareness and analysis of fraud risk that may be present within Cooperative operations. Leadership should be in a constant mode of analyzing the risks associated with the performance, recording, and reporting of financial transactions. Thus, the fraud risk assessment process, as its name implies, identifies those areas of financial transaction processing and reporting with the greatest risks of fraud.

The information that follows is presented to address the “how to” of the *documentation* of a fraud risk assessment process:

Guidelines for a Formal Fraud Risk Assessment

The standard objective of a fraud risk assessment is not to prevent fraud, but rather to determine what “frauds” need to be prevented. These identified fraud risks are then used as a focus of where new internal control activities / processes should be directed.

A properly designed fraud risk assessment includes appointing a team that includes a representative from each functional area of the Cooperative (billing, accounting, human resources, etc.). This team is charged with the responsibility of asking and answering the questions...

“How can someone steal (misappropriate funds) from our Cooperative?”

“How can someone misstate our financial statements?”

This type of brainstorming session will breed a discussion that results in the identification of fraud risks. The process does not need to be any more difficult than this.

Once the fraud risks are identified, those risks should be documented in written form for submission to those responsible for development of new internal controls to address these identified risks.

Recommendation

Consideration should be given to performing formal fraud risk assessments on a periodic schedule that addresses each area of Cooperative operations at least once every two years. To facilitate the performance and documentation of the process, we have provided the following exhibits:

Exhibit F1 – Fraud Risk Assessment Tool

This document is a 35-page questionnaire that assists in breeding discussion within the fraud risk assessment team meeting(s).

Exhibit F2 – Fraud Risk Assessment Framework

This form is used to formally document the fraud risks identified in the team meeting(s) for submission to those responsible for the development of new internal controls.

We remain available to assist with future implementation of the Fraud Risk Assessment process as needed.

JEMEZ MOUNTAINS ELECTRIC COOPERATIVE, INC.

INTERNAL CONTROL PROCESS CONSULTATION Executive Summary

DOCUMENTATION OF INTERNAL CONTROLS / ANTI-FRAUD PROGRAM

Section G

This section is provided for your reference and future use since this engagement does not include creating the documentation of the anti-fraud program.

The purpose in properly documenting internal controls included in an anti-fraud program is to ensure continuity in the application of controls over an extended time period. Over time, staff may not recall the intricacies of the controls in place and thus it becomes watered-down, or less than effective. Over time, as new employees are trained, some of the intricacies of the controls may not be communicated in their entirety, thus rendering the design of the control ineffective.

Previously in this Report, we provided the recommendation that all processes in place regarding accounting and transaction processing be committed to written form as “process documentation”. However, the recommendations addressed in this section include the overall documentation of internal controls included in the anti-fraud program rather than the aforementioned process documentation.

This documentation should be simple, yet complete. The information that follows represents our recommendations regarding the process of documenting an anti-fraud program.

Recommendations

The documentation of the anti-fraud program should begin with an overall introduction which includes the purpose of the program. The narrative includes information that can be used in the periodic Cooperative-wide fraud awareness training that is recommended in the following section.

An example of this documentation is provided below:

JEMEZ MOUNTAINS ELECTRIC COOPERATIVE, INC. Company Anti-Fraud Program
<p style="text-align: center;"><i>Introduction</i></p> <p>The Board of Trustees, Audit Committee, and Management of Jemez Mountains Electric Cooperative, Inc. (the “Cooperative”), has established this program to address the risk of occurrences of internal fraud. Internal fraud is defined as fraud perpetrated against the Cooperative by our own people. The purpose also includes the establishment of an environment that promotes and recognizes honesty and integrity in the workforce, and a safe and pleasant working atmosphere.</p> <p>Internal fraud includes three types of fraud: Misappropriation, Corruption, and Financial Statement Fraud, illustrated as follows:</p> <p><i>Misappropriation:</i> This is defined as the taking of cooperative assets whether cash, inventory, or other fixed assets. This is the most common type of fraud.</p> <p><i>Corruption:</i> This type of fraud is represented by collusion between at least two individuals (one employee and a non-employee, or two employees) that includes conflicts of interest in purchasing and sales schemes; bribery in kickbacks and bid-rigging schemes; illegal gratuities; and economic extortion.</p> <p><i>Financial Statement Fraud:</i> This fraud includes the intentional misrepresentation of the financial position or results of operations of the Cooperative.</p>

JEMEZ MOUNTAINS ELECTRIC COOPERATIVE, INC.

INTERNAL CONTROL PROCESS CONSULTATION Executive Summary

DOCUMENTATION OF INTERNAL CONTROLS / ANTI-FRAUD PROGRAM

Section G

The Introduction continues as follows:

This Anti-Fraud Program, through the collective efforts of the Board of Trustees, Audit Committee, and Management has been developed to address the risk of internal fraud. The contents of this Anti-Fraud Program are required to be in written form. As such, this Anti-Fraud Program documentation is intended as the complete documentation necessary to evidence the Program.

Management is responsible for documenting all aspects of this Program. Upon completion of the various documentation forms (fraud risk assessment framework, control activities forms), the responsible parties shall forward that information to management for the assembly into this formal Anti-Fraud Program.

The communication of and staff training for this Program is conducted periodically. However, the Program is available at all times on the Cooperative intranet and is provided to each employee whether through printed form or through electronic distribution through the Cooperative email system.

The next section includes an introduction to the existence of policies that address the risk of internal fraud.

Policies of Protection

Certain policies have been established that provide protection for not only the Cooperative, but for each employee as well. On the date of employment, each employee will receive an Employee Handbook that includes the complete text of Cooperative policies. As relates to fraud, the following policies have been adopted:

Code of Ethics

Our Cooperative is committed to conducting our business with the highest level of integrity. We have adopted this Code to set expectations of ethical performance of job functions, and to exhibit to the general public and our members our commitment to excellence in service provision.

Fraud Policy / Fraud Reporting Policy

We want you to know that we take the issue of internal fraud seriously. We have adopted a “no tolerance” position regarding fraud occurrences and desire that the workforce joins us in this level of dedication to fraud prevention and detection. This policy was adopted to provide information about fraud, what to do if you suspect fraud, and our obligations to investigate suspicions of fraud. The policy also outlines the administrative actions that will be applied if you are suspected of the perpetration of internal fraud.

This policy provides you the opportunity to anonymously report suspicions of fraud. A healthy workforce environment is the result of you feeling as if you have someone to turn to in reporting suspicions. The policy outlines the process to follow in reporting any suspicions and our responsibilities to investigate these issues.

JEMEZ MOUNTAINS ELECTRIC COOPERATIVE, INC.

INTERNAL CONTROL PROCESS CONSULTATION Executive Summary

DOCUMENTATION OF INTERNAL CONTROLS / ANTI-FRAUD PROGRAM

Section G

Program documentation continues with outlining the purposes and processes related to the Fraud Risk Assessment Process.

Fraud Risk Assessment

Introduction

A formal fraud risk assessment process is required by this Anti-Fraud Program. The fraud risk assessment is to be performed periodically by the Fraud Risk Assessment Team as identified below.

The purpose of the fraud risk assessment process is to identify those areas of transaction performance and recording that are most vulnerable to fraud. Control activities to address these identified areas are developed by the Control Activities Development Team as identified in the Control Activities section of this program.

Fraud Risk Assessment Team

The fraud risk assessment team shall include staff positions from various areas within the Cooperative such as:

- Management (Executive and Middle)
- Chief Financial Officer
- Controller
- Human Resources
- Billing / Purchasing
- Customer Service
- Construction / Engineering

The Fraud Risk Assessment shall be documented utilizing the Fraud Risk Assessment Framework included as Appendix A to this Program.

Once completed, the Fraud Risk Assessment Framework shall be provided to the Control Activities Development Team to serve as a guide for the performance of their responsibilities as defined.

The risk assessment team should remain aware of operational changes that could result in additional vulnerabilities to fraud.

The facilitator of the risk assessment team shall inform executive management of any new vulnerabilities that may be identified in-between fraud risk assessments. Executive management has the responsibility to present these new vulnerabilities to the Control Activities Development Team for inclusion in the Anti-Fraud Program if determined necessary.

JEMEZ MOUNTAINS ELECTRIC COOPERATIVE, INC.

INTERNAL CONTROL PROCESS CONSULTATION Executive Summary

DOCUMENTATION OF INTERNAL CONTROLS / ANTI-FRAUD PROGRAM

Section G

In keeping with the framework of the six elements of an anti-fraud program, Control Activities are presented:

Control Activities

Introduction

Control Activities are defined as those activities, controls, checks, and balances, and processes that have been implemented to address the risks of internal fraud in our Cooperative.

A Control Activity can be as simple as the requirement for two authorized signatures on checks over a certain dollar amount, to as complex as a complete policy such as the Expense Reimbursement Policy.

Control Activities Development Team

The Control Activities Development Team shall include at least the following staff positions:

Executive Management
Chief Financial Officer
Controller

Upon receipt of the Fraud Risk Assessment Framework, the team shall develop certain and specific Control Activities that address the identified fraud risks. Control Activities shall be documented using the Control Activities form included as Appendix B to this Program.

Communication of Control Activities

The complete Anti-Fraud Program, including Specific Control Activities will be issued in its entirety at the bi-annual deadline of June 1st utilizing the following means of communication:

Electronic Distribution: Cooperative Intranet, Email
Print Distribution: As a part of this Anti-Fraud Program
Continuous Training: As directed by this Program

The level of communication and training related to Control Activities will be conducted to ensure a thorough understanding of the requirements imposed upon all staff positions.

Compliance with Control Activities

Control Activities have been developed over time with an extensive amount of effort. It is required that Control Activities applying to your specific position will be followed. We encourage staff to ask questions if there is a lack of understanding of any Control Activity. Failure to adhere to the various Control Activities will result in the following:

First Violation: Formal reprimand, and re-training if necessary
Second Violation: Termination

As a part of the on-going Monitoring aspect of this Program, we encourage you to submit to the Control Activities Development Team any suggestions you may have for improving specific Control Activities.

Specific Control Activities

Specific Control Activities that have been placed into operation are included as Appendix C to this Program.

JEMEZ MOUNTAINS ELECTRIC COOPERATIVE, INC.

INTERNAL CONTROL PROCESS CONSULTATION Executive Summary

DOCUMENTATION OF INTERNAL CONTROLS / ANTI-FRAUD PROGRAM

Section G

The information presented above represents the narrative portion of documenting the anti-fraud program.

Included as **Exhibit G1** to this Report is a sample Control Activities Documentation Form that can be used to document the specific control activities that have been placed in operation. This is a generic sample and thus does not purport to represent the control activities placed in operation for Jemez Mountains Electric Cooperative, Inc.

JEMEZ MOUNTAINS ELECTRIC COOPERATIVE, INC.

INTERNAL CONTROL PROCESS CONSULTATION Executive Summary

COMMUNICATION: ANTI-FRAUD PROGRAM / FRAUD AWARENESS TRAINING

Section H

A properly functioning anti-fraud program includes a regular schedule of Cooperative-wide anti-fraud training. Based on the needs of the Cooperative, this training can be conducted monthly, quarterly, semi-annually, and/or annually.

Recommendations

At a minimum, training regarding new or revised policies, along with training related to the operation of new or revised internal control processes should be conducted. This provides an increase in the level of fraud awareness, which results in an increase in the perception of detection.

The risk associated with fictitious vendors and/or man-in-the-middle attacks has increased exponentially over the past several years. We believe that targeted training on spearfishing, phishing, man-in-the-middle attacks, and social engineering should be a part of future Cooperative-wide training.

The Cooperative should establish a formal Cooperative-wide training program that includes the following:

- Overall Anti-Fraud Program Review (Every two years)
- Annual Review and Re-signature of Fraud-related Policies and the Conflict of Interest Form
- Periodic (monthly or quarterly)
 - Fraud Definition
 - Fraud Types
 - Fraud Trends
 - Fraud Costs
 - Industry-Specific Fraud Issues
 - Fraud Indicators for the Cooperative
 - Suggestions for Improvements in Control Activities

Communication also includes how fraud risks, internal controls, and overall fraud prevention processes are communicated to the Board of Trustees. Of the six elements of anti-fraud program design, the Board of Trustees is responsible for establishing the environment (foundational policies) and then directing certain other management employees to carry out the administration of these policies and to require a reporting on the effectiveness of these directives. As presented previously, the position that performs these internal audit related procedures should prepare and present this report. This “reporting” is addressed in the Monitoring and Routine Maintenance Section of this Report.

JEMEZ MOUNTAINS ELECTRIC COOPERATIVE, INC.

INTERNAL CONTROL PROCESS CONSULTATION Executive Summary

COMMUNICATION: ANTI-FRAUD PROGRAM / FRAUD AWARENESS TRAINING

Section H

For use as a reference tool, included as **Exhibit H1** is a three-page document produced by the Association of Certified Fraud Examiners that provides considerations for organizations when going through the process of establishing an effective Company-wide anti-fraud training program.

JEMEZ MOUNTAINS ELECTRIC COOPERATIVE, INC.

INTERNAL CONTROL PROCESS CONSULTATION Executive Summary

MONITORING AND ROUTINE MAINTENANCE

Section I

Increasing the perception of detection is a leading objective of an effective monitoring program. Monitoring of the operation and effectiveness of internal controls leads to increasing this perception of detection.

The monitoring element includes two primary “question” areas as follows:

1. How are the controls working out?

Through the testing of compliance with existing internal controls, the effectiveness of the control can be assessed. In some circumstances, problems can be categorized as a human problem (adherence to the control) or a design problem, or both. In any circumstance, employees can be re-trained to address the human problem, and controls can be modified to address the design problem.

2. What employee input can we obtain into the proper functioning or design of the anti-fraud program?

Obtaining the involvement of employees in the monitoring process then serves to obtain their “buy-in” of the overall fraud prevention process. It is noted that buy-in is a continuous process since change is a continuous process.

The addition of a formal monitoring structure can only serve to strengthen the overall control structure. The performance of certain Internal Audit Related Procedures as has been presented in this Report represents a major part of the Monitoring process.

Recommendations

The Cooperative should consider the establishment of this formal Monitoring / Routine Maintenance process.

Periodic meetings with employees should occur that solicits answers to the two question areas of a monitoring system. These meetings can include a review of the compliance audit programs and working papers to breed discussion on any modifications that need to be made to the existing internal controls. As a result, Control Activities documentation can be amended and thus kept current as part of the overall anti-fraud program.

Another by-product of these meetings is a workforce that understands the “whys” of processes, the “hows” of processes, and establishes ownership in the processes. With ownership of the process, the desired outcome is that the employee becomes less likely to violate the process through the committing of internal fraud.

The Cooperative should consider implementing the performance of internal audit related procedures as recommended previously in this Report.

JEMEZ MOUNTAINS ELECTRIC COOPERATIVE, INC.

INTERNAL CONTROL PROCESS CONSULTATION Executive Summary

MONITORING AND ROUTINE MAINTENANCE

Section I

Exhibit I1 – Compliance Audit Program, and **Exhibit I2** – Compliance Audit Workpaper represent samples that can be used to document the performance of compliance reviews as a part of the performance of the internal audit related procedures.

Once completed, a formal written report to the Board of Trustees, Audit Committee, and Management should be prepared. This can be referred to as an “Internal Control Report”, an “Anti-Fraud Program Report” or any similar type of name as determined best fits the nature of Cooperative operations.

Issues that may be addressed in this type of reporting are as follows:

- New controls / control processes implemented and an explanation of the reasons for their establishment
- Results of compliance audit procedures performed during the most recent reporting period
- Revisions of existing controls / control processes and an explanation of the reasons for the modification
- Training – addressing fraud awareness and/or fraud risks specific to the Cooperative
- Informing or updating on instances of internal fraud discovered at the Cooperative

Included as **Exhibit I3** is a sample reporting format that can be used to accomplish this reporting objective.

JEMEZ MOUNTAINS ELECTRIC COOPERATIVE, INC.

INTERNAL CONTROL PROCESS CONSULTATION Executive Summary

COMPLETION ISSUES

We remain available to advise on drafts of new policies or existing policy revisions in conjunction with your legal counsel.

We remain available to conduct the training necessary to communicate new or revised policies and procedures to the workforce as determined necessary by the management team.

As stated in this Report, we desire this engagement to be the start of a continuing relationship that provides Cooperative staff with the ability to consult with us as needed as operations change and as new control issues arise. As an example, if the Cooperative develops wholesale ACH payment processes for vendor payments as a replacement for the writing of checks, this will create the need for advice on specific controls necessary for electronic payment versus hard copy check payment.

It should also be understood that the implementation of the processes and recommendations included in this Report will be a lengthy process that occurs over a period of several years. As such, the atmosphere of a continuing relationship is not only helpful, but necessary.

Throughout this Report we have stated that we remain available to assist the Cooperative with implementation of the various recommendations. We believe that much of the value of an internal control process consultation is realized after the issuance of the Report. As such, the issuance of this Report is intended to represent a beginning, rather than a completion of the consulting process. We encourage you to view this process in this manner in order to maximize the benefit received from this engagement.

EXHIBIT D1

Sample Code of Ethics

SAMPLE CODE OF ETHICS

***SHOULD NOT BE ADOPTED UNTIL REVIEWED AND APPROVED
BY CORPORATE LEGAL COUNSEL***

Purpose

To ensure that all directors, officers, and staff conduct the business of [Company Name] in an honest and ethical manner in order to best serve the interest of [Company Name] and its members.

This policy has been developed to provide guidelines to the directors, officers, and staff of the Company in order that in the performance of their duties, confidence and respect may be promoted within the membership of the Company and the communities where the Company serves. This policy is not intended to be an all-inclusive document because situations will always exist where individuals must exercise their own judgment and rely upon their own sense of what constitutes ethical conduct.

The guidelines contained in this Code are issues of common sense. The sound judgment and continuing concern of directors, officers, and staff for their integrity, and the trust and confidence of the membership, will always be the single most important guideline when dealing with questions of ethics and appropriate conduct.

Fair Competition

The Company supports competition based on quality, service, and price. We will conduct our affairs honestly, directly, and fairly. To that end, employees,

- Must never discuss with competitors any matter directly involving competition (e.g. sales prices, marketing strategies, policies)
- Must never agree with a competitor to restrict competition by fixing prices, allocating markets, or by other means)
- Must be accurate and truthful in all dealings with members.

Conflicts of Interest

There are several situations that could give rise to a conflict of interest. The most common are accepting gifts from suppliers, employment by another company, ownership of a significant part of another company or business, close or family relationships with outside suppliers, and communications with competitors. A potential conflict of interest exists for employees who make decisions in their jobs that would allow them to give preference or favor to a member in exchange for anything of personal benefit to themselves or their friends and families.

Our policy is that employees will not do business on behalf of the Company for which a conflict of interest exists. However, recognizing that these transactions sometimes do occur, they must be reported on the Conflict of Interest Form.

Annually, each employee will review the Code of Ethics, sign the code's Acknowledgment section, and complete the Conflict of Interest Form.

SAMPLE CODE OF ETHICS

***SHOULD NOT BE ADOPTED UNTIL REVIEWED AND APPROVED
BY CORPORATE LEGAL COUNSEL***

Gifts

No employee or member of his immediate family shall solicit or accept from an actual or prospective customer or supplier any compensation, advance loans, gifts, entertainment, or other favors which are of more than token value (e.g. \$100). Under no circumstances should a gift or entertainment be accepted which would influence the employee's judgment.

Any employee who receives, or whose family member receives, an unsolicited prohibited gift, should report it to his supervisor and should return it to the person making the gift.

Entertainment and services offered by a supplier or customer may be accepted by an employee when they are associated with a business meeting and the supplier or customer provides them to others as a normal part of its business.

Outside Employment

Employees must not be employed outside the Company:

- In any business that competes with Company,
- In a manner which would affect their objectivity in carrying out their responsibilities, and/or
- Where the outside employment would conflict with scheduled hours or the performance of their job responsibilities.

Confidential Information

Confidential information includes all information, whether technical, business, financial or otherwise concerning the Company which the Company treats as confidential or secret, and/or which is not available or is not made available publicly. It also includes any private information of, or relating to, customer records, fellow employees, other persons or other companies obtained by virtue of the employee's position.

Confidential information must not be divulged to any outside party. This prohibition exists during and continues after employment with the Company.

Reporting Violations

All employees are responsible for compliance with this Code. Each employee has an obligation to the Company that transcends normal reporting relationships. Employees should be alert to possible violations of the Code and are encouraged to report such violations promptly to the employee's supervisor, the appropriate security, audit, or legal department personnel, or elsewhere as the circumstance dictates.

Confidentiality will be maintained throughout the investigative process to the extent consistent with adequate investigation. The Company will not allow retaliation of any kind against individuals making good faith reports of violations of this Code of Ethics.

SAMPLE CODE OF ETHICS

***SHOULD NOT BE ADOPTED UNTIL REVIEWED AND APPROVED
BY CORPORATE LEGAL COUNSEL***

Discipline

Violations of this Code can result in serious consequences for the Company, its image, credibility, and confidence of its members and can include fines and restrictions on future Company operations. Accordingly, disciplinary action may include:

- Reprimand
- Probation
- Suspension
- Demotion
- Termination

Acknowledgement and Signature

I have read and understand the contents of this Code of Ethics and agree to abide by the provisions of this Code.

Signature

Date

EXHIBIT D2

Sample Fraud / Fraud Reporting Policy

SAMPLE FRAUD / FRAUD REPORTING POLICY

***SHOULD NOT BE ADOPTED UNTIL REVIEWED AND APPROVED
BY CORPORATE LEGAL COUNSEL***

Policy Statement

The {Board of Directors / Owners} of _____ are responsible for the prevention and detection of fraud. All parties should be familiar with the types of fraud that might occur and should be alert for any indication of fraud. This policy has been established to provide a framework for the treatment of suspicions of fraud and for reporting suspicions of fraud. {Company Name} commits to properly addressing the concerns of employees as submitted in accordance with the provisions of this policy.

Scope

This policy applies equally to any fraudulent activity involving not only employees but also directors, vendors, and/or outside agencies, without regard to length of service, title/position, or relationship. It is understood that these parties may make a report of suspicions of fraud under this policy.

Reportable Actions Constituting Fraud

The terms fraud, misappropriation, and irregularities are synonymous terms commonly used to refer to occupational or internal fraud. There are three types of fraud: Asset Misappropriation (the taking of company assets), Corruption (collusion between at least two parties to gain personally while causing a loss to the company), and Financial Statement Fraud (misrepresenting the financial position and/or results of operations).

Fraud can include, but is not limited to any dishonest act, misapplication of funds or assets, profiting on insider knowledge, destruction of records or assets, disclosure of confidential information, forgery or alteration of documents, impropriety in reporting transactions, gifts from vendors (outside of limits), disappearance of records or assets, and/or any similar or related irregularity.

Predication (Reasonable Cause)

The Company has implemented this policy to encourage the reporting of suspicions that fraud is occurring or has been perpetrated against the organization. It is understood that in making a report in accordance with this policy, proof positive evidence is not necessary. The potential reporter does not have to be right. The potential reporter should simply consider what predication, or reasonable cause, exists to make a report.

Accordingly, those considering making a report under this policy should provide some type of documentation that a fraud may have been committed or at least indicate that the specific issue may appear to be fraudulent in nature. It is the responsibility of the investigators to form the conclusion that presentable fraud has occurred. Maliciously false or frivolous reports made under this policy will be dealt with in accordance with the whistleblower provisions of this Policy.

Any individual making a notification must be acting in good faith and have reasonable grounds for believing the information provided. Allegations made maliciously or with knowledge of their falsity will not be tolerated. In no circumstance should an individual confront the fraud suspect or attempt his/her own investigation.

SAMPLE FRAUD / FRAUD REPORTING POLICY

***SHOULD NOT BE ADOPTED UNTIL REVIEWED AND APPROVED
BY CORPORATE LEGAL COUNSEL***

Reporting Structure (Tailor to your organization, e.g. Committee Reporting, External Fraud Hotline)

The {board of directors}, of the organization have established a formal reporting mechanism whereby any individual who has knowledge of any suspected fraudulent activity can anonymously report these suspicions.

The reporting process is as follows: {the remainder of this section will provide the details of the selected processes of reporting}

Non-fraud Irregularities

Identification or allegations of personal improprieties or irregularities whether moral or behavioral, should be resolved by departmental management, executive management, and/or the human resources department, rather than audit related departments or agencies.

Investigation Responsibilities

Upon receipt of the notification of alleged fraudulent activities, management and the board of directors will investigate the specific allegations utilizing available internal and/or external resources. The parties shall retain in their possession all documentation regarding the nature of the allegations, the date the allegations were received, the resolution of the allegations, and the date resolved. Decisions to refer investigation results to the appropriate authorities for prosecution will be made in conjunction with legal counsel, the board of directors, and senior management.

Authorization for Investigation

Those individuals or agencies assigned the responsibility for investigation may take control of and gain full access to the organization's records and premises without prior consent of any individual who may have custody of any such records or facilities.

Whistleblower Protection

Employees may not retaliate against a whistleblower for reporting an activity which that person believes to be fraudulent or dishonest. Retaliation can be evidenced by the intent of adversely affecting the terms or conditions of employment (including, but not limited to, threats of physical harm, dismissal, transfer to an undesirable job assignment, demotion, suspension, or impact on salary or wages). The whistleblower is defined as a party who reports allegations of fraud in accordance with the provisions of this Policy. Whistleblowers who believe that they have been retaliated against may file a written complaint with {responsible party such as corporate legal counsel}. Any complaint of retaliation will be promptly investigated by the {responsible party} and appropriate measures will be taken if allegations of retaliation are proven. This protection from retaliation is not intended to prohibit managers or supervisors from taking action, including disciplinary action, in the usual scope of their duties and based on valid performance-related factors.

SAMPLE FRAUD / FRAUD REPORTING POLICY

***SHOULD NOT BE ADOPTED UNTIL REVIEWED AND APPROVED
BY CORPORATE LEGAL COUNSEL***

Suspension/Termination

During an investigation, the suspected individual may be suspended with pay. Based upon the results of the investigation, the individual will either be reinstated or terminated under the direction of organizational legal counsel. Fraudulent activities will be prosecuted to the fullest extent of the law.

Acknowledgement and Signature

I have read the contents of this fraud policy. I understand that management will not tolerate fraudulent or dishonest activities of any kind and that I am not to engage in such acts while employed by

_____.

Signature

Date

EXHIBIT D3

Presumption of Privacy Policy Example Provisions

Presumption of Privacy Policy Example Provisions

“To facilitate the performance of employees’ job functions, employees will be provided with a proper workspace, including but not limited to the following: Desks, file cabinets, credenzas, and other office document hard copy storage furniture. All items on location in these assigned workspaces, including any personal effects stored on Company property, will be subject to search as determined necessary, and employees have no reasonable expectation of privacy in these workspaces”.

“To facilitate business communications and work-related research, the Company provides staff access to various types of communications equipment, including but not limited to the following: Internet, phones and voice mail, wireless devices, computers and related equipment, and email.

All materials, information and/or software created, transmitted, downloaded or stored on these Company-provided means of communication are the property of the Company, and employees have no reasonable expectation of privacy in such information”.

EXHIBIT D4

Anti-Bribery / Anti-Corruption Policy

ANTI-BRIBERY / ANTI-CORRUPTION POLICY

***SHOULD NOT BE ADOPTED UNTIL REVIEWED AND APPROVED
BY CORPORATE LEGAL COUNSEL***

Purpose

The purpose of this policy is to establish controls to ensure compliance with all applicable anti-bribery and corruption regulations, and to ensure that the Company's business is conducted in a socially responsible manner.

Policy Statement

Bribery is the offering, promising, giving, accepting, or soliciting of an advantage as an inducement for action which is illegal or a breach of trust. A bribe is an inducement or reward offered, promised or provided in order to gain any commercial, contractual, regulatory, or personal advantage.

It is our policy to conduct all of our business in an honest and ethical manner. We take a zero- tolerance approach to bribery and corruption. We are committed to acting professionally, fairly and with integrity in all our business dealings and relationships wherever we operate and implementing and enforcing effective systems to counter bribery. We will uphold all laws relevant to countering bribery and corruption in all the jurisdictions in which we operate.

Scope

In this policy, third party means any individual or organization you come into contact with during the course of your work for us, and includes actual and potential clients, customers, suppliers, distributors, business contacts, agents, advisers, and government and public bodies, including their advisors, representatives and officials, politicians, and political parties.

This policy applies to all individuals working at all levels and grades, including senior managers, officers, directors, employees (whether permanent, fixed-term or temporary), consultants, contractors, trainees, remote workers, casual workers and agency staff, volunteers, interns, agents, sponsors, or any other person associated with us (collectively referred to as employees in this policy).

This policy covers:

- Bribes;
- Gifts and hospitality;
- Facilitation payments;
- Political contributions;
- Charitable contributions.

Bribes

Employees must not engage in any form of bribery, either directly or through any third party (such as an agent or distributor).

Gifts and hospitality

Employees must not offer or give any gift or hospitality:

- which could be regarded as illegal or improper, or which violates the recipient's policies;

ANTI-BRIBERY / ANTI-CORRUPTION POLICY

***SHOULD NOT BE ADOPTED UNTIL REVIEWED AND APPROVED
BY CORPORATE LEGAL COUNSEL***

- or to any public employee or government officials or representatives, or politicians or political parties;
- or which exceeds \$100 in value for each individual gift, or \$500 in value for each hospitality event (not to exceed a total value of \$1,000 in any financial year), unless approved in writing by the employee's manager.

Employees may not accept any gift or hospitality from our business partners if:

- it exceeds \$100 in value for each individual gift, or \$500 in value for each hospitality event (not to exceed a total of \$1,000 in any financial year), unless approved in writing by the employee's manager; or
- it is in cash; or
- there is any suggestion that a return favor will be expected or implied.

If it is not appropriate to decline the offer of a gift, the gift may be accepted, provided it is then declared to the employee's manager and donated to charity.

The test to be applied is whether in all the circumstances the gift or hospitality is reasonable and justifiable. The intention behind the gift should always be considered. Where this policy requires written approval to be given, the General Manager shall put in place a process to maintain a register of all such approvals.

Facilitation payments and kickbacks

Facilitation payments are a form of bribery made for the purpose of expediting or facilitating the performance of a public official for a routine governmental action, and not to obtain or retain business or any improper business advantage. Facilitation payments tend to be demanded by low level officials to obtain a level of service which one would normally be entitled to.

Our strict policy is that facilitation payments must not be paid. We recognize, however, that our employees may be faced with situations where there is a risk to the personal security of an employee or his/her family and where a facilitation payment is unavoidable, in which case the following steps must be taken:

- Keep any amount to the minimum;
- Create a record concerning the payment; and
- Report it to your supervisor.

In order to achieve our aim of not making any facilitation payments, each business of the Company will keep a record of all payments made, which must be reported to the General Manager in order to evaluate the business risk and to develop a strategy to minimize such payments in the future.

Political Contributions

We do not make donations, whether in cash or kind, in support of any political parties or candidates, as this can be perceived as an attempt to gain an improper business advantage.

ANTI-BRIBERY / ANTI-CORRUPTION POLICY

***SHOULD NOT BE ADOPTED UNTIL REVIEWED AND APPROVED
BY CORPORATE LEGAL COUNSEL***

Charitable contributions

Charitable support and donations are acceptable (and indeed are encouraged), whether of in-kind services, knowledge, time, or direct financial contributions. However, employees must be careful to ensure that charitable contributions are not used as a scheme to conceal bribery. We only make charitable donations that are legal and ethical under local laws and practices. No donation must be offered or made without the prior approval of the General Manager.

Your responsibilities

You must ensure that you read, understand, and comply with this policy.

The prevention, detection and reporting of bribery and other forms of corruption are the responsibility of all those working for us or under our control. All employees are required to avoid any activity that might lead to, or suggest, a breach of this policy.

You must notify your supervisor as soon as possible if you believe or suspect that a conflict with or breach of this policy has occurred, or may occur in the future.

Any employee who breaches this policy will face disciplinary action, which could result in dismissal for gross misconduct. We reserve our right to terminate our contractual relationship with other workers if they breach this policy.

Record-keeping

We must keep financial records and have appropriate internal controls in place which will evidence the business reason for making payments to third parties.

You must declare and keep a written record of all hospitality or gifts accepted or offered, which will be subject to managerial review.

You must ensure all expenses claimed relating to hospitality or gifts are submitted in accordance with our expense policy and specifically record the reason for the expenditure.

All accounts, invoices, memoranda and other documents and records relating to dealings with third parties, such as clients, suppliers, and business contacts, should be prepared and maintained with strict accuracy and completeness. No accounts must be kept "off-book" to facilitate or conceal improper payments.

How to raise a concern

You are encouraged to raise concerns about any issue or suspicion of malpractice at the earliest possible stage. If you are unsure whether a particular act constitutes bribery or corruption, or if you have any other questions or concerns, these should be raised with your supervisor.

What to do if you are a victim of bribery or corruption

ANTI-BRIBERY / ANTI-CORRUPTION POLICY

***SHOULD NOT BE ADOPTED UNTIL REVIEWED AND APPROVED
BY CORPORATE LEGAL COUNSEL***

It is important that you inform your supervisor as soon as possible if you are offered a bribe by a third party, are asked to make one, suspect that this may happen in the future, or believe that you are a victim of another form of unlawful activity.

Whistleblower Protection

Employees who refuse to accept or offer a bribe, or those who raise concerns or report another's wrongdoing, are sometimes worried about possible repercussions. We aim to encourage openness and will support anyone who raises genuine concerns in good faith under this policy, even if they turn out to be mistaken.

We are committed to ensuring no one suffers any detrimental treatment as a result of refusing to take part in bribery or corruption, or because of reporting in good faith their suspicion that an actual or potential bribery or other corruption offence has taken place, or may take place in the future. Detrimental treatment includes dismissal, disciplinary action, threats, or other unfavorable treatment connected with raising a concern. If you believe that you have suffered any such treatment, you should inform your supervisor immediately. If the matter is not remedied, and you are an employee, you should raise it formally using the company's Grievance Procedure.

Training and communication

Training on this policy forms part of the orientation process for all new employees. All existing employees will receive regular, relevant training on how to implement and adhere to this policy. In addition, all employees will be asked to formally accept conformance to this policy on an annual basis.

Our zero-tolerance approach to bribery and corruption must be communicated to all suppliers, contractors and business partners at the outset of our business relationship with them and as appropriate thereafter.

Who is responsible for the policy?

The board of directors has overall responsibility for ensuring this policy complies with our legal and ethical obligations, and that all those under our control comply with it. The general manager has primary and day-to-day responsibility for implementing this policy, and for monitoring its use and effectiveness and dealing with any questions on its interpretation. Management at all levels are responsible for ensuring those reporting to them are made aware of and understand this policy and are given adequate and regular training on it.

Monitoring and review

The General Manager will monitor the effectiveness and review the implementation of this policy, regularly considering its suitability, adequacy, and effectiveness. Any improvements identified will be made as soon as possible. Internal control systems and procedures will be subject to regular audits to provide assurance that they are effective in countering bribery and corruption.

All employees are responsible for the success of this policy and should ensure they use it to disclose any suspected danger or wrongdoing.

ANTI-BRIBERY / ANTI-CORRUPTION POLICY

***SHOULD NOT BE ADOPTED UNTIL REVIEWED AND APPROVED
BY CORPORATE LEGAL COUNSEL***

Employees are invited to comment on this policy and suggest ways in which it might be improved. Comments, suggestions and questions should be addressed to the General Manager.

Acknowledgement

EXHIBIT E1

New Vendor Establishment Form

Company Name

New Vendor Establishment

Vendor Information								Validation Procedures							
Vendor Information								Documents or Procedures Performed							
Vendor Name:															
Taxpayer ID#:															
Payee Name:															
Duplicate Name Search:															
Primary Phone:															
Fax No.:															
Website:															
<u>Physical Address:</u>															
Address:															
City:															
State:															
Zip Code:															
<u>Mailing Address:</u>															
Address:															
City:															
State:															
Zip Code:															
Duplicate Address Search:															
Contact Person:															
Contact E-mail:															
<u>Payment Information</u>															
Bank Name:															
Bank Routing Number:															
Bank Account Number:															
ACH Authorization On File:															
<u>Company Personnel Relationships with Vendor (conflicts of interest):</u>															
VIC Code:														aBc123	

EXHIBIT E2

Existing Vendor Information Change Form

Company Name

Existing Vendor Information Change

Vendor Information	Changed From:	Changed To:	VIC Code Verified
Vendor Name:			
Taxpayer ID#:			
Payee Name:			
Vendor Information Changed:			
Phone No:			
Fax No:			
Website:			
<u>Physical Address:</u>			
Address:			
City:			
State:			
Zip Code:			
<u>Mailing Address:</u>			
Address:			
City:			
State:			
Zip Code:			
Contact Person:			
Contact E-mail:			
<u>Payment Information</u>			
Bank Name:			
Bank Routing Number:			
Bank Account Number:			
ACH Authorization On File:			

EXHIBIT E3

Sample Conflict of Interest Form

Company Name
Conflict of Interest Form

To be completed annually by all employees, owners, and members of the governing body. If there are any questions as to what category a relationship should be included, select one and management shall determine any necessary reclassifications.

Name: _____
Title: _____

Signature

Please provide individual names, company names, and the nature of the relationships that may exist with organizations that our company does business with or that you could reasonably expect our company could potentially enter into a relationship with, as relates to:

Family Relationships:

Personal Relationships:

Business Relationships:

Financial Relationships:

EXHIBIT E4

Benford's Law – Presentation/Training Extract



DATA ANALYTICS

Data Analytics

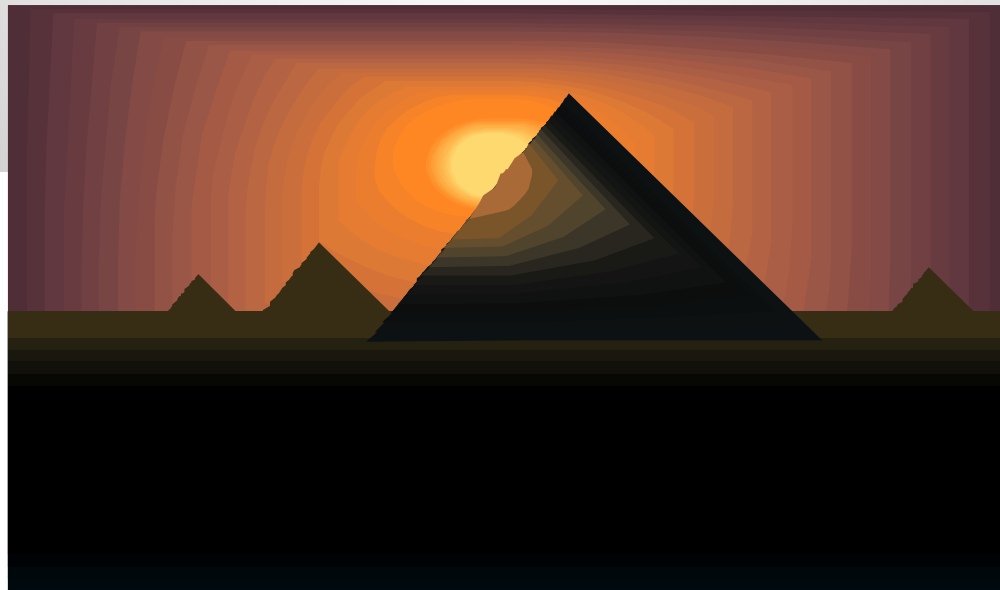
Use of data-mining to analyze data for...

- ❑ Red-flags**
- ❑ Anomalies**
- ❑ Deviations from Expectations**

BENFORD'S LAW

The “Magic” Fraud Detection Tool

The Origin of Benford's Law



The Origin of Benford's Law

Simon Newcomb (1881):

Astronomer, Mathematician

Logarithm Book: Used to multiply large numbers before calculators and computers

The Origin of Benford's Law

Simon Newcomb (1881):

Observed that the first few pages of the logarithm book were more worn and dirtier than the other pages

The Origin of Benford's Law

Simon Newcomb (1881):

The first few pages lists multi-digit logs beginning with 1, 2, and 3.

Newcomb theorized that scientists spent more time dealing with logs that began with 1, 2, or 3, and that for each succeeding number, the amount of time decreased.

The Origin of Benford's Law

Frank Benford (1938):

Physicist employed by General Electric

While looking at his logarithm book, Benford noticed the exact same phenomena as Newcomb

The Origin of Benford's Law

Frank Benford (1938):

Benford tested his theory and then developed the logarithmic formula for Benford's Law

The Origin of Benford's Law

Frank Benford (1938):

The theory has never been disproved

However, the practical application of Benford's Law was still not known

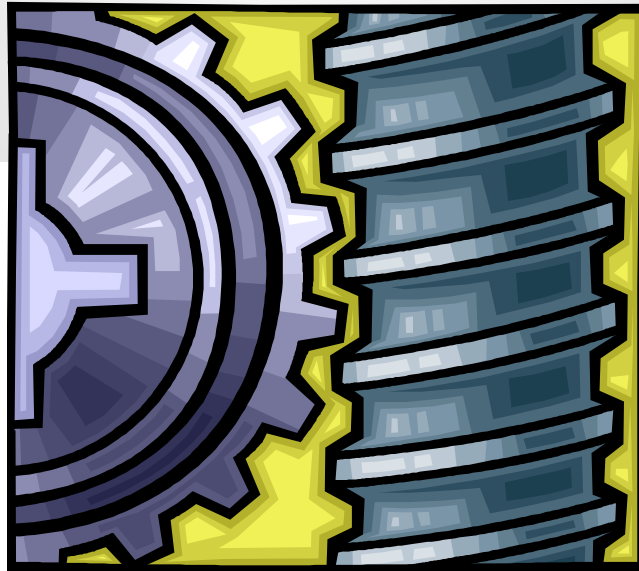
The Origin of Benford's Law

1970s - Benford's Law could be used to test the financial reasonableness of forecasts

1980s - Used to detect the reasonableness of rounded numbers - Determined that invented numbers do not conform to the Law

1990s - Mark Nigrini developed the use for detecting fraud

How Benford's Law Works



How Benford's Law Works

THE LAWS OF THE "LAW"

Sample size must be large enough that the numbers can manifest themselves

Cannot use randomly generated numbers (lottery tickets) – Each number is designed to have an equal chance of getting picked

How Benford's Law Works

THE LAWS OF THE "LAW"

Will not work with non-naturally occurring numbers

Social Security Numbers

Telephone Numbers

Drivers License Numbers

How Benford's Law Works

Mark Nigrini, Ph. D. – Southern Methodist University

Invented Numbers are not Natural

**Invented Numbers will not likely follow
Benford's Law**

How Benford's Law Works

Mark Nigrini, Ph. D. – Southern Methodist University

The Law can be used to analyze the digital frequencies of data sets to identify potential fraudulent items

The Law can be used to identify possible inefficiencies

How Benford's Law Works

Fraudsters conceal activities by approving disbursements just below review limits – thus a digital anomaly will occur

How Benford's Law Works

Nigrini's 5 Tests

1st Digit Test:

High level review that will identify obvious anomalies

Will point you in the right direction

How Benford's Law Works

Nigrini's 5 Tests

2nd Digit Test:

High level review that also will identify obvious anomalies

How Benford's Law Works

Nigrini's 5 Tests

First Two Digits Test:

More focused

Can be used to select audit samples

How Benford's Law Works

Nigrini's 5 Tests

First Three Digits Test:

Even More focused

Can be used to further refine audit samples

Can identify overused digit patterns indicative of fraud, or duplicate processing of invoices

How Benford's Law Works

Nigrini's 5 Tests

Last Two Digits Test:

Used to identify invented (overused) and rounded numbers

How Benford's Law Works

Nigrini's Rules for Data Sets:

Data sets should describe similar data

Town Populations

Stock Market Quotes

How Benford's Law Works

Nigrini's Rules for Data Sets:

Artificial limits should be non-existent

No pre-set minimums or maximums

How Benford's Law Works

Nigrini's Rules for Data Sets:

Data set cannot be numbers that are pre-arranged

Phone Numbers

Social Security Numbers

How Benford's Law Works

Nigrini's Rules for Data Sets:

Data set should not be a subset of a set

Data should not represent aggregated totals

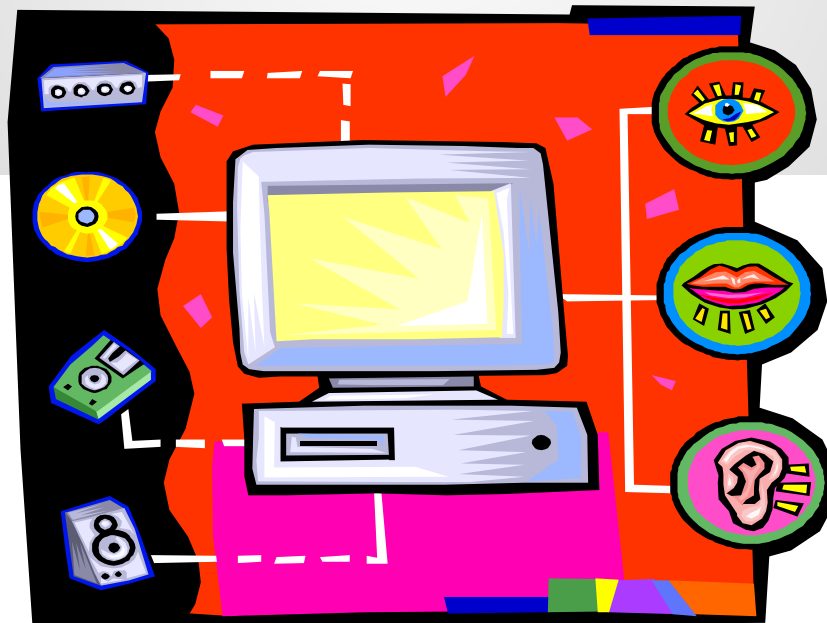
Accounting data should relate to a specific accounting period

How Benford's Law Works

Nigrini's Rules for Data Sets:

Data set should be large enough so that the expected proportions can be manifested

Practical Applications of Benford's Law



BENFORD'S LAW ANALYSIS						
Raw Data						
Check #	Amount	Payee	First Digit	First 2 Digits		
4001	225.95	SEIU .	2	22		
4002	1,212.97	S. ELEV CORP.	1	12		
4003	4,999.50	YORK INT CORP.	4	49		
4004	339.13	US FOODSERVICE CUST 3.	3	33	1	352 32.18%
4005	473.98	VDT OF TAXATION	4	47	2	153 13.99%
4006	250.81	W W GRAINGER INC	2	25	3	157 14.35%
4007	504.00	LJC LIGHTING SUPPLY	5	50	4	136 12.43%
4008	171.70	CLERK, DC SUPERIOR COURT	1	17	5	74 6.76%
4009	225.15	SEIU	2	22	6	47 4.30%
4010	477.26	VDT OF TAXATION	4	47	7	52 4.75%
4011	6,438.54	MD COMPTROLLR	6	64	8	72 6.58%
4012	481.28	AMERICAN AIR FILTER	4	48	9	51 4.66%
4013	3,457.33	ARAMARK CAFÉ	3	34		1094 100.00%
4014	224.22	OEIU LU 99 DUES	2	22		
4015	94.53	HOME PARAMOUNT	9	94	10	42 0.03839
4016	186.39	BLAYDES INDUSTRIES INC	1	18	11	48 0.04388
4017	219.54	MONARCH PAINT AND WALLCOVERING CO	2	21	12	32 0.02925
4018	346.16	Oxenburg's INC	3	34	13	57 0.0521
4019	1,714.24	DC TREASURER	1	17	14	19 0.01737
4020	315.14	WASHINGTON PAPER & CHEMICAL	3	31	15	53 0.04845
4021	385.51	US FOODSERVICE	3	38	16	29 0.02651
4022	4,319.01	MD COMPTROLLR OF TREASURY	4	43	17	24 0.02194
4023	1,500.00	GARCIA'S	1	15	18	37 0.03382
4024	353.00	Grants	3	35	19	11 0.01005
4025	6,374.79	MD COMPTROLLR OF TREASURY	6	63	20	21 0.0192
4026	272.37	HOME PARAMOUNT PEST CONTROL CO.	2	27	21	8 0.00731
4027	1,419.86	STATE STREET BANK & TRUST	1	14	22	31 0.02834
4028	424.70	OTTENBERG'S BAKERY	4	42	23	30 0.02742
4029	2,403.95	MD COMPTROLLR OF TREASURY	2	24	24	11 0.01005
4030	775.00	THORNTON SERVICE.	7	77	25	19 0.01737
4031	303.00	AQUATOMIC PRODUCTS	3	30	26	9 0.00823
4032	4,613.49	SMEKINSON-SYSCO	4	46	27	6 0.00548

BENFORD'S LAW ANALYSIS							
Raw Data							
Check #	Amount	Payee	First Digit	First 2 Digits			
4033	373.01	Lyles	3	37	28	8	0.00731
4034	7,857.80	S & W CONTROLS INC	7	78	29	10	0.00914
4035	32,000.48	Pepco Inc Inc	3	32	30	41	0.03748
4036	61,421.13	Pepco Inc Inc	6	61	31	18	0.01645
4037	1,591.25	STATE STREET BANK & TRUST	1	15	32	11	0.01005
4038	16.45	ROBERTS COMPANY	1	16	33	6	0.00548
4039	1,179.35	STATE STREET BANK & TRUST	1	11	34	14	0.0128
4040	306.50	MAURICE ELECTRICAL SUPPLY	3	30	35	15	0.01371
4041	36,655.25	Pepco Inc Inc	3	36	36	10	0.00914
4042	298.08	US FOODSERVICE	2	29	37	16	0.01463
4043	2,243.77	WASHINGTON GAS	2	22	38	5	0.00457
4044	157.56	JAC IUOE	1	15	39	21	0.0192
4045	738.94	CAREY'S CLEANERS	7	73	40	10	0.00914
4046	25.25	JOHNSON CONTROLS	2	25	41	10	0.00914
4047	1,206.95	ELEVATOR CONTROLL SERVICE	1	12	42	12	0.01097
4048	3,303.85	WASHINGTON GAS	3	33	43	17	0.01554
4049	137.57	HOME DEPOT/GECF	1	13	44	7	0.0064
4050	1,959.22	WASHINGTON GAS	1	19	45	5	0.00457
4051	80.60	METROCALL #116940	8	80	46	8	0.00731
4052	1,581.32	STATE STREET BANK & TRUST	1	15	47	23	0.02102
4053	1,212.97	SCHINDLER ELEV CORP	1	12	48	25	0.02285
4054	395.20	US FOOD SERVICE	3	39	49	19	0.01737
4055	157.56	JAC IUOE	1	15	50	20	0.01828
4056	412.08	SERV EMP INTL	4	41	51	11	0.01005
4057	237.23	ALLIED PLYWOOD CORP	2	23	52	10	0.00914
4058	388.31	COMPLETE AIR FILTER - MISC SUPPLIES 1/8/99.	3	38	53	9	0.00823
4059	232.81	INTL UNION OF OPER ENGINRS LU 99-99A	2	23	54	7	0.0064
4060	1,700.92	DC TREASURER	1	17	55	1	0.00091
4061	106.81	AMERICAN WINDOW & BLDG CLEANING	1	10	56	3	0.00274
4062	1,363.50	Grants	1	13	57	1	0.00091
4063	234.83	SEIU	2	23	58	5	0.00457

BENFORD'S LAW ANALYSIS							
Raw Data							
Check #	Amount	Payee	First Digit	First 2 Digits			
4064	1,607.16	STATE STREET BANK & TRUST	1	16	59	7	0.0064
4065	3.45	HOME DEPOT/GE CF	3	34	60	10	0.00914
4066	534.45	US FOODSERVICE	5	53	61	8	0.00731
4067	255.82	BLAYDES INDUSTRIES INC	2	25	62	6	0.00548
4068	484.00	US FOODSERVICE	4	48	63	1	0.00091
4069	300.00	AQUATOMIC RODUCTS	3	30	64	1	0.00091
4070	1,648.27	DC WATER & SEWER AUTHORITY	1	16	65	1	0.00091
4071	188.97	SHENANDOAH S PRIDE	1	18	66	4	0.00366
4072	536.84	VDT OF TAXATION	5	53	67	3	0.00274
4073	106.81	AMERICAN WINDOW & BLDG CLEANING	1	10	68	6	0.00548
4074	399.89	J A SEXAUER, INC	3	39	69	7	0.0064
4075	225.84	W W GRAINGER INC	2	22	70	7	0.0064
4076	1,978.81	WASHINGTON GAS	1	19	71	4	0.00366
4077	60.85	BFPE INTERNATIONAL	6	60	72	2	0.00183
4078	222.00	OEIU LU 99 DUES	2	22	73	2	0.00183
4079	1,500.00	GARCIA'S	1	15	74	2	0.00183
4080	156.00	JAC IUOE	1	15	75	1	0.00091
4081	133.24	MAURICE ELECTRICAL SUPPLY	1	13	76	1	0.00091
4082	230.98	SEIU - LU	2	23	77	11	0.01005
4083	291.29	US FOODSERVI CE	2	29	78	13	0.01188
4084	305.22	MONARCH PAINT AND WALLCOVERING CO	3	30	79	9	0.00823
4085	71.92	ROBERTS COMPANY	7	71	80	5	0.00457
4086	530.25	TECHNICAL INSPECTION INC	5	53	81	4	0.00366
4087	309.57	MAURICE ELECTRICAL SUPPLY	3	30	82	5	0.00457
4088	93.59	HOME PARAMOUNT PEST CONTROL CO	9	93	83	3	0.00274
4089	1,816.80	GARCIA'S INC	1	18	84	2	0.00183
4090	283.04	US FOODSERVICE	2	28	85	3	0.00274
4091	1,816.80	GARCIA'S INC	1	18	86	4	0.00366
4092	477.64	WASHINGTON PAPER & CHEMICAL	4	47	87	45	0.04113
4093	139.84	CLERK, DC SUPERIOR COURT	1	13	88	0	0
4094	707.81	BFPE INTERNATIONAL	7	70	89	1	0.00091
4095	101.00	FED RESERV RICHMOND	1	10	90	3	0.00274

BENFORD'S LAW ANALYSIS							
Raw Data							
Check #	Amount	Payee	First Digit	First 2 Digits			
4096	303.00	AQUATOMIC RODUCTS	3	30	91	1	0.00091
4097	54.73	DOOR CLOSER SERVICE CO INC	5	54	92	1	0.00091
4098	300.00	DMV ELEVATOR INSP INC	3	30	93	17	0.01554
4099	469.77	US FOODSERVICE	4	46	94	19	0.01737
4100	499.73	WASHINGTON PAPER & CHEMICAL	4	49	95	3	0.00274
4101	2,525.00	DC TREASURER	2	25	96	3	0.00274
4102	285.87	US FOODSERVICE	2	28	97	2	0.00183
4103	87.59	ALLEN BUSINESS MACHINES	8	87	98	1	0.00091
4104	286.73	ALLIED PLYWOOD CORP	2	28	99	1	0.00091
4105	418.14	SERV EMP INTL UN LU 82	4	41		1094	100.00%
4106	374.00	SERV EMP INTL UN LU 82	3	37			
4107	490.21	VDT OF TAXATION	4	49			
4108	105.75	AMERICAN WINDOW & BLDG CLEANING	1	10			
4109	498.81	US FOODSERVICE #3923000	4	49			
4110	283.89	ALLIED PLYWOOD CORP	2	28			
4111	208.28	H M SWEENEY CO	2	20			
4112	303.00	D M V ELEVATORS INSP INC	3	30			
4113	1,345.80	WASHINGTON PAPER & CHEMICAL	1	13			
4114	3,006.15	DC WATER & SEWER AUTHORITY	3	30			
4115	101.00	FEDERAL RESERVE BANK OF RICHMOND	1	10			
4116	2,293.90	ARAMARK CAFÉ	2	22			
4117	80.60	METROCALL ACCT 116940	8	80			
4118	1,212.97	SCHINDLER ELEV CORP	1	12			
4119	614.20	G C S SVC INC	6	61			
4120	1,206.95	ELEVATOR CONTROL SERVICE	1	12			
4121	487.37	VOID	4	48			
4122	18.79	ROBERTS OXYGEN CO	1	18			
4123	162.50	EROL'S SUPPLIES	1	16			
4124	19.40	HOME DEPOT/GECF	1	19			
4125	1,281.24	STATE STREET BANK & TRUST	1	12			
4126	433.74	ADAMS-BURCH INC	4	43			
4127	268.16	E.C. CUSH CO	2	26			

BENFORD'S LAW ANALYSIS

1st Digit Results

Record
Count

1094

First Digit	Expected Frequency Count	Expected Frequency Percent	Actual Frequency Count	Difference	Actual Percentage Frequency	Difference
1	329	30.10%	352	23	32.18%	2.08%
2	193	17.60%	153	-40	13.99%	-3.61%
3	137	12.50%	157	20	14.35%	1.85%
4	106	9.70%	136	30	12.43%	2.73%
5	86	7.90%	74	-12	6.76%	-1.14%
6	73	6.70%	47	-26	4.30%	-2.40%
7	63	5.80%	52	-11	4.75%	-1.05%
8	56	5.10%	72	16	6.58%	1.48%
9	50	4.60%	51	1	4.66%	0.06%

BENFORD'S LAW ANALYSIS
1st Two Digits Results

**Record
Count**

1094

First Two Digits	Expected Frequency Count	Expected Frequency Percent	Actual Frequency Count	Difference	Actual Percentage Frequency	Difference
10	45	4.14%	42	-3	3.84%	-0.30%
11	41	3.78%	48	7	4.39%	0.61%
12	38	3.48%	32	-6	2.93%	-0.55%
13	35	3.22%	57	22	5.21%	1.99%
14	33	3.00%	19	-14	1.74%	-1.26%
15	31	2.80%	53	22	4.84%	2.04%
16	29	2.63%	29	0	2.65%	0.02%
17	27	2.48%	24	-3	2.19%	-0.29%
18	26	2.35%	37	11	3.38%	1.03%
19	24	2.23%	11	-13	1.01%	-1.22%
20	23	2.12%	21	-2	1.92%	-0.20%
21	22	2.02%	8	-14	0.73%	-1.29%
22	21	1.93%	31	10	2.83%	0.90%
23	20	1.85%	30	10	2.74%	0.89%
24	19	1.77%	11	-8	1.01%	-0.76%
25	19	1.70%	19	0	1.74%	0.04%
26	18	1.64%	9	-9	0.82%	-0.82%
27	17	1.58%	6	-11	0.55%	-1.03%
28	17	1.52%	8	-9	0.73%	-0.79%
29	16	1.47%	10	-6	0.91%	-0.56%
30	16	1.42%	41	25	3.75%	2.33%
31	15	1.38%	18	3	1.65%	0.27%
32	15	1.34%	11	-4	1.01%	-0.33%

First Two Digits	Expected Frequency Count	Expected Frequency Percent	Actual Frequency Count	Difference	Actual Percentage Frequency	Difference
33	14	1.30%	6	-8	0.55%	-0.75%
34	14	1.26%	14	0	1.28%	0.02%
35	13	1.22%	15	2	1.37%	0.15%
36	13	1.19%	10	-3	0.91%	-0.28%
37	13	1.16%	16	3	1.46%	0.30%
38	12	1.13%	5	-7	0.46%	-0.67%
39	12	1.10%	21	9	1.92%	0.82%
40	12	1.07%	10	-2	0.91%	-0.16%
41	11	1.05%	10	-1	0.91%	-0.14%
42	11	1.02%	12	1	1.10%	0.08%
43	11	1.00%	17	6	1.55%	0.55%
44	11	0.98%	7	-4	0.64%	-0.34%
45	11	0.96%	5	-6	0.46%	-0.50%
46	10	0.93%	8	-2	0.73%	-0.20%
47	10	0.91%	23	13	2.10%	1.19%
48	10	0.90%	25	15	2.29%	1.39%
49	10	0.88%	19	9	1.74%	0.86%
50	9	0.86%	20	11	1.83%	0.97%
51	9	0.84%	11	2	1.01%	0.17%
52	9	0.83%	10	1	0.91%	0.08%
53	9	0.81%	9	0	0.82%	0.01%
54	9	0.80%	7	-2	0.64%	-0.16%
55	9	0.78%	1	-8	0.09%	-0.69%
56	8	0.77%	3	-5	0.27%	-0.50%
57	8	0.76%	1	-7	0.09%	-0.67%
58	8	0.74%	5	-3	0.46%	-0.28%
59	8	0.73%	7	-1	0.64%	-0.09%
60	8	0.72%	10	2	0.91%	0.19%
61	8	0.71%	8	0	0.73%	0.02%
62	8	0.70%	6	-2	0.55%	-0.15%
63	7	0.68%	1	-6	0.09%	-0.59%
64	7	0.67%	1	-6	0.09%	-0.58%

First Two Digits	Expected Frequency Count	Expected Frequency Percent	Actual Frequency Count	Difference	Actual Percentage Frequency	Difference
65	7	0.66%	1	-6	0.09%	-0.57%
66	7	0.65%	4	-3	0.37%	-0.28%
67	7	0.64%	3	-4	0.27%	-0.37%
68	7	0.63%	6	-1	0.55%	-0.08%
69	7	0.63%	7	0	0.64%	0.01%
70	7	0.62%	7	0	0.64%	0.02%
71	7	0.61%	4	-3	0.37%	-0.24%
72	7	0.60%	2	-5	0.18%	-0.42%
73	6	0.59%	2	-4	0.18%	-0.41%
74	6	0.58%	2	-4	0.18%	-0.40%
75	6	0.58%	1	-5	0.09%	-0.49%
76	6	0.57%	1	-5	0.09%	-0.48%
77	6	0.56%	11	5	1.01%	0.45%
78	6	0.55%	13	7	1.19%	0.64%
79	6	0.55%	9	3	0.82%	0.27%
80	6	0.54%	5	-1	0.46%	-0.08%
81	6	0.53%	4	-2	0.37%	-0.16%
82	6	0.53%	5	-1	0.46%	-0.07%
83	6	0.52%	3	-3	0.27%	-0.25%
84	6	0.51%	2	-4	0.18%	-0.33%
85	6	0.51%	3	-3	0.27%	-0.24%
86	5	0.50%	4	-1	0.37%	-0.13%
87	5	0.50%	45	40	4.11%	3.61%
88	5	0.49%	0	-5	0.00%	-0.49%
89	5	0.49%	1	-4	0.09%	-0.40%
90	5	0.48%	3	-2	0.27%	-0.21%
91	5	0.48%	1	-4	0.09%	-0.39%
92	5	0.47%	1	-4	0.09%	-0.38%
93	5	0.46%	17	12	1.55%	1.09%
94	5	0.46%	19	14	1.74%	1.28%
95	5	0.46%	3	-2	0.27%	-0.19%
96	5	0.45%	3	-2	0.27%	-0.18%

First Two Digits	Expected Frequency Count	Expected Frequency Percent	Actual Frequency Count	Difference	Actual Percentage Frequency	Difference
97	5	0.45%	2	-3	0.18%	-0.27%
98	5	0.44%	1	-4	0.09%	-0.35%
99	5	0.44%	1	-4	0.09%	-0.35%

List of Invoices/Payees to Examine Benford's Law - 1st Two Digits Test

<u>Check</u> <u>#</u>	<u>Amount</u>	<u>Payee</u>
4132	87.75	GK Lee, Inc.
4149	87.75	GK Lee, Inc.
4167	87.75	GK Lee, Inc.
4188	87.75	GK Lee, Inc.
4204	87.75	GK Lee, Inc.
4219	87.75	GK Lee, Inc.
4226	87.75	GK Lee, Inc.
4237	87.75	GK Lee, Inc.
4239	87.75	GK Lee, Inc.
4250	87.75	GK Lee, Inc.
4259	87.75	GK Lee, Inc.
4263	87.75	GK Lee, Inc.
4296	87.75	GK Lee, Inc.
4300	87.75	GK Lee, Inc.
4318	87.75	GK Lee, Inc.
4350	87.75	GK Lee, Inc.
4375	87.75	GK Lee, Inc.
4429	87.75	GK Lee, Inc.
4528	87.75	GK Lee, Inc.
4562	87.75	GK Lee, Inc.
4643	87.75	GK Lee, Inc.
4646	87.75	GK Lee, Inc.
4648	87.75	GK Lee, Inc.
4706	87.75	GK Lee, Inc.
4707	87.75	GK Lee, Inc.
4756	87.75	GK Lee, Inc.
4773	87.75	GK Lee, Inc.
4779	87.75	GK Lee, Inc.
4803	87.75	GK Lee, Inc.
4831	87.75	GK Lee, Inc.
4837	87.75	GK Lee, Inc.
4856	87.75	GK Lee, Inc.
4878	87.75	GK Lee, Inc.
4881	87.75	GK Lee, Inc.
4888	87.75	GK Lee, Inc.
4909	87.75	GK Lee, Inc.
4923	87.75	GK Lee, Inc.

List of Invoices/Payees to Examine Benford's Law - 1st Two Digits Test

<u>Check</u> <u>#</u>	<u>Amount</u>	<u>Payee</u>
4976	87.75	GK Lee, Inc.
4997	87.75	GK Lee, Inc.
5027	87.75	GK Lee, Inc.
5033	87.75	GK Lee, Inc.
5080	87.75	GK Lee, Inc.
4023	1,500.00	GARCIA'S
4079	1,500.00	GARCIA'S
4131	1,500.00	GARCIA'S
4143	1,500.00	GARCIA'S
4271	1,500.00	GARCIA'S
4309	1,500.00	GARCIA'S
4378	1,500.00	GARCIA'S
4397	1,500.00	GARCIA'S
4424	1,500.00	GARCIA'S
4519	1,500.00	GARCIA'S
4552	1,500.00	GARCIA'S
4610	1,500.00	GARCIA'S
4873	1,500.00	GARCIA'S
4948	1,500.00	GARCIA'S
5034	1,500.00	GARCIA'S
5056	1,500.00	GARCIA'S
5071	1,500.00	GARCIA'S
4199	1,798.81	GARCIA'S INC
4865	1,798.81	GARCIA'S INC
4091	1,816.80	GARCIA'S INC
4764	1,816.80	GARCIA'S INC
4163	1,798.81	GARCIA'S INC
4252	1,798.81	GARCIA'S INC
4444	1,798.81	GARCIA'S INC
4544	1,798.81	GARCIA'S INC
4616	1,798.81	GARCIA'S INC
4797	1,798.81	GARCIA'S INC
4979	1,798.81	GARCIA'S INC
4089	1,816.80	GARCIA'S INC
4147	1,816.80	GARCIA'S INC

List of Invoices/Payees to Examine Benford's Law - 1st Two Digits Test

<u>Check</u> <u>#</u>	<u>Amount</u>	<u>Payee</u>
4446	1,816.80	GARCIA'S INC
4601	1,816.80	GARCIA'S INC
4744	1,816.80	GARCIA'S INC
4867	1,816.80	GARCIA'S INC
4991	1,816.80	GARCIA'S INC
4453	1,798.81	GARCIA'S INC.
4288	1,816.80	GARCIA'S INC.

EXHIBIT F1

Fraud Risk Assessment Tool

MODULE 1 - Employee Assessment

These questions are designed to assess the probability of a fraudulent event occurring based on: Internal Controls, the Internal Control Environment and, Resources to Prevent, Detect, and Deter Fraud

Item #	Procedure	Yes	No	Comments
1.	Are employees provided formal written job descriptions?			
2.	Are employees provided with an organizational chart that shows lines of responsibility?			
3.	Does the company have written accounting policies and procedures?			
4.	Is there a formal policy covering approval authority for financial transactions, such as purchasing or travel?			
5.	Does the company have an ethics statement?			
6.	Does senior management exhibit and encourage ethical behavior?			
7.	Does the company have a written fraud policy?			
8.	Is a senior member of management responsible for compliance with fraud policies?			
9.	Does the company educate employees about the importance of ethics and anti-fraud programs?			
10.	Does the company provide an anonymous way to report suspected violations of the ethics and anti-fraud programs?			
11.	Are fraud incidents promptly and thoroughly investigated?			
12.	Does the company maintain a record of fraud incidents?			
13.	Does the company conduct pre-employment background checks?			

MODULE 1 - Employee Assessment

These questions are designed to assess the probability of a fraudulent event occurring based on: Internal Controls, the Internal Control Environment and, Resources to Prevent, Detect, and Deter Fraud

Item #	Procedure	Yes	No	Comments
14.	Does the company have a loss prevention function?			
15.	Does the company have an internal audit function?			
16.	Are the duties related to authorization, custody of assets, and recording or reporting of transactions segregated?			
17.	Is compliance with internal controls audited periodically?			
18.	Do employees feel they are treated and compensated fairly?			
19.	Do any employees have large personal debts or credit problems?			
20.	Do any employees appear to be spending far more than they are earning?			
21.	Do any employees gamble excessively?			
22.	Do any employees use alcohol or drugs excessively?			
23.	Do any employees resent their superiors?			
24.	Do any employees have a close relationship with vendors or competitors?			
25.	Do any employees have outside business interests that might conflict with their duties at the company?			
26.	Is the company experiencing high employee turnover?			
27.	Are employees required to take vacations annually?			

MODULE 1 - Employee Assessment

These questions are designed to assess the probability of a fraudulent event occurring based on: Internal Controls, the Internal Control Environment and, Resources to Prevent, Detect, and Deter Fraud

Item #	Procedure	Yes	No	Comments
28.	Is the company dominated by a small group of individuals?			
29.	Does the company have unrealistic productivity measurements and expectations?			
30.	Does management fail to give employees positive feedback and recognition for job performance?			
31.	Are employees afraid to deliver bad news to supervisors or management?			
32.	Is there a lack of communication between employees and management?			
33.	Is there a lack of clear organizational responsibilities in the company?			
34.	Does management not seem to care about or reward appropriate employee behavior?			

MODULE 2 - Management / Key Employee Assessment

These questions are designed to assess the probability of a fraudulent event occurring based on: Internal Controls, the Internal Control Environment and, Resources to Prevent, Detect, and Deter Fraud

Item #	Procedure	Yes	No	Comments
1.	Is the board of directors composed of mainly officers of the company or related individuals?			
2.	Is there an independent audit committee?			
3.	Has there been high turnover of managers and members of the board of directors?			
4.	Have an unusually high number of employees left the company recently?			
5.	Is the company involved in any litigation?			
6.	Does the company have offshore activities or bank accounts?			
7.	Do any of senior management have offshore bank accounts or business interests?			
8.	Are any key employees experiencing financial pressures such as debts, gambling, medical bills, or divorce?			
9.	Do any key employees appear to be living beyond their means?			
10.	Do any key employees have civil judgments or bankruptcies on record?			
11.	Do any key employees have a criminal conviction?			
12.	Do one or two key employees appear to dominate the company?			

MODULE 2 - Management / Key Employee Assessment

These questions are designed to assess the probability of a fraudulent event occurring based on: Internal Controls, the Internal Control Environment and, Resources to Prevent, Detect, and Deter Fraud

Item #	Procedure	Yes	No	Comments
13.	Do any key employees have friends or relatives reporting directly to them?			
14.	Do any of the key employees appear to have a close association with a vendor?			
15.	Do any key employees have outside business interests that might conflict with their duties at the company?			
16.	Do any key employees own a portion of any company that does business with this company?			
17.	Has any key employee failed to take vacation?			
18.	Do any key employees have a significant amount of their net worth invested in the company?			
19.	Does the company have unusually high debts?			
20.	Is key employee compensation primarily based on company performance?			
21.	Is there an incentive to use inappropriate means to minimize earnings for tax reasons?			
22.	Is there excessive pressure to increase the company's stock price?			
23.	Has the company recently experienced large operating or investment losses?			
24.	Does the organization have sufficient working capital?			

MODULE 2 - Management / Key Employee Assessment

These questions are designed to assess the probability of a fraudulent event occurring based on: Internal Controls, the Internal Control Environment and, Resources to Prevent, Detect, and Deter Fraud

Item #	Procedure	Yes	No	Comments
25.	Does the organization have sufficient credit?			
26.	Is the company under pressure to report favorable earnings?			
27.	Does the company depend heavily on only a limited number of products or customers?			
28.	Has the company experienced difficulty in collecting receivables?			
29.	Has the company recently expanded rapidly into new business or product lines?			
30.	Has the company experienced a reduction in sales volume?			
31.	Does the company have strong competitors that are outperforming?			
32.	Is the company under pressure to sell or merge with another company?			
33.	Does the company change auditors often?			
34.	Does the company delay or avoid supplying auditors with the information necessary to complete the audits?			
35.	Does the company have problems with regulatory agencies?			
36.	Does the company have poor accounting records?			
37.	Does the accounting department appear to be inadequately staffed?			

MODULE 2 - Management / Key Employee Assessment

These questions are designed to assess the probability of a fraudulent event occurring based on: Internal Controls, the Internal Control Environment and, Resources to Prevent, Detect, and Deter Fraud

Item #	Procedure	Yes	No	Comments
38.	Does the organization fail to disclose questionable or unusual accounting practices?			
39.	Does the company have a number of large year-end or unusual transactions?			
40.	Does the organization lack an adequate internal audit staff?			
41.	Does the organization lack an internal control system, or does it fail to enforce the existing internal controls?			

MODULE 3 - Physical Controls to Deter Employee Theft and Fraud

These assessment questions are designed to assess the probability of a fraudulent event occurring based on: Physical Controls in place to control access to accounting records and information and, physical controls in place to protect company assets.

Item #	Procedure	Yes	No	Comments
1.	Does the organization conduct pre-employment background checks to identify previous dishonest or unethical behavior?			
2.	Are there policies and procedures that address dishonest or unethical behavior?			
3.	Does management support the ethics and anti-fraud policies?			
4.	Does the organization educate employees about the importance of ethics and anti-fraud programs?			
5.	Does the organization provide an anonymous way to report suspected violations of the ethics and anti-fraud policies?			
6.	Does the organization restrict access to areas containing sensitive documents (such as invoices, receipts, journals, ledgers, and checks) and maintain a system for providing an audit trail of access?			
7.	Does the organization restrict access to computer systems with sensitive documents (such as accounting software, inventory, and payroll) and create a system to provide an audit trail of access?			
8.	Does the organization restrict access to areas with high value assets, such as shipping, receiving, storerooms, and cash?			
9.	Does the organization use CCTV and recording equipment to monitor entries, exits, areas with sensitive or high value assets, and sales areas?			
10.	Does the organization conduct random, unannounced audits of inventory, cash, expense, purchasing, billing, and other accounts by internal or external auditors?			

MODULE 3 - Physical Controls to Deter Employee Theft and Fraud

These assessment questions are designed to assess the probability of a fraudulent event occurring based on: Physical Controls in place to control access to accounting records and information and, physical controls in place to protect company assets.

Item #	Procedure	Yes	No	Comments
11.	Does the organization use professional loss prevention or security personnel to monitor physical controls?			
12.	Does the organization promptly investigate incidents of suspected or reported fraud?			

MODULE 4 - Skimming Schemes

Skimming schemes include: 1) collecting cash, but not recording the sale, 2) collecting cash, keep a portion of the cash, and underreporting the sale amount, 3) collecting a customer's payment, but not crediting the amount to the customer's account and 4) collecting cash and holding it in a personal interest-bearing account before depositing it into the company account

Item #	Procedure	Yes	No	Comments
1.	Is there periodic analytical review of sales accounts using vertical, horizontal, and ratio analysis?			
2.	Is there periodic review of the inventory and receiving records using statistical sampling?			
3.	Is there periodic review of the inventory and receiving records using trend analysis?			
4.	Is there periodic review of the inventory and receiving records using physical inventory counts?			
5.	Is there periodic review of the inventory and receiving records using verification of shipping and requisition documents?			
6.	Is there periodic review of inventory accounts for write-off?			
7.	Is there periodic review of accounts receivable and allowance for uncollectible accounts to look for write-offs of accounts receivable?			
8.	Is there periodic review of cash accounts for irregular entries?			
9.	Is the company mail opened by someone other than bookkeepers, cashiers, or other accounting employees who make journal entries?			
10.	Do vouchers for credit and sales receipts contain serial numbers?			
11.	Is the accounts receivable bookkeeper restricted from preparing the bank deposit?			
12.	Is the accounts receivable bookkeeper restricted from collecting cash from customers?			

MODULE 4 - Skimming Schemes

Skimming schemes include: 1) collecting cash, but not recording the sale, 2) collecting cash, keep a portion of the cash, and underreporting the sale amount, 3) collecting a customer's payment, but not crediting the amount to the customer's account and 4) collecting cash and holding it in a personal interest-bearing account before depositing it into the company account

Item #	Procedure	Yes	No	Comments
13.	Is the accounts receivable bookkeeper restricted from access to the cash receipts?			
14.	Is the cashier restricted from accessing accounts receivable records?			
15.	Is the cashier restricted from accessing bank and customer statements?			
16.	Is each of the following responsibilities assigned to a separate employee: general ledger entries, cash receipt entries and, accounts receivable billing?			
17.	Does the employee who opens incoming checks place restrictive endorsements on all checks received?			
18.	Does the person who opens the mail prepare a list of all checks and cash received?			
19.	Does the person who opens the mail deliver all checks and cash to the person responsible for the daily bank deposit?			
20.	Does an employee perform an independent verification of the bank deposit ticket to the remittance list generated by the employee who opened the mail?			
21.	Does the company use a lockbox service for cash receipts?			
22.	Does the company have a safe with restricted access?			
23.	Is cash deposited daily?			
24.	Are there pre-numbered cash receipts for sales?			

MODULE 4 - Skimming Schemes

Skimming schemes include: 1) collecting cash, but not recording the sale, 2) collecting cash, keep a portion of the cash, and underreporting the sale amount, 3) collecting a customer's payment, but not crediting the amount to the customer's account and 4) collecting cash and holding it in a personal interest-bearing account before depositing it into the company account

Item #	Procedure	Yes	No	Comments
25.	Are employees who handle cash bonded?			
26.	Is there a written policy and procedure for turning over delinquent accounts for collection?			
27.	Is the person who handles customer complaints independent of the cashier or accounts receivable function?			
28.	Is physical access to the accounting system restricted to only authorized persons?			

MODULE 5 - Cash Larceny Schemes

Cash Larceny Schemes include: 1) stealing cash at the point of sale or register, 2) stealing cash receipts posted to sales and receivable journals, 3) stealing cash from bank deposits

Item #	Procedure	Yes	No	Comments
1.	Are cash register tape totals reconciled to the amount in the cash drawer?			
2.	Is an employee other than the register worker responsible for preparing register count sheets and agreeing them to register totals?			
3.	Is access to registers or the cash box closely monitored? Are access codes kept secure?			
4.	Are customer complaints regarding short change or improper posting handled by someone other than the employee who receives the cash?			
5.	Are register workers properly supervised?			
6.	Are CCTV cameras and digital recorders used to monitor register areas?			
7.	Is each receivable transaction reviewed for legitimacy and supporting documentation?			
8.	Is an independent listing of cash receipts prepared before the receipts are submitted to the cashier or accounts receivable bookkeeper?			
9.	Does a person independent of the cash receipts and accounts receivable functions compare entries to the cash receipts journals with the bank deposit slips and bank deposit statements?			
10.	Are the cash receipts, cash counts, bank deposits, deposit receipt reconciliations, bank reconciliations, posting of deposits, and cash disbursements duties segregated?			
11.	Does an employee other than the cashier or accounts receivable bookkeeper make the daily bank deposit?			

MODULE 5 - Cash Larceny Schemes

Cash Larceny Schemes include: 1) stealing cash at the point of sale or register, 2) stealing cash receipts posted to sales and receivable journals, 3) stealing cash from bank deposits

Item #	Procedure	Yes	No	Comments
12.	Is job or assignment rotation mandatory for employees who handle cash receipts and accounting duties?			
13.	Are vacations mandatory for employees who handle cash receipts and accounting duties?			
14.	Are surprise cash counts conducted?			
15.	Are journal entries made to the cash accounts reviewed and analyzed on a regular basis?			
16.	Does the company use a point of sale (POS) system?			
17.	Does the POS system track perpetual inventory?			
18.	Does the POS system track exceptions, such as voids, refunds, no sales, overages, and shortages?			
19.	Are register exception reports reviewed on a regular basis?			
20.	Are all employees, except for managers, prohibited from making changes to the POS system?			
21.	Is access to the accounts receivable subledger and the general ledger restricted to authorized employees? Does access leave an audit trail?			

MODULE 6 - Check Tampering Schemes

Check Tampering Schemes Include: 1) forged maker schemes involve forging an authorized signature on a company check, 2) forged endorsements schemes consist of forging the signature endorsement of an intended recipient of a company check, 3) Altered payee schemes involve changing the payee designation on the check to the perpetrator or an accomplice, 4) Authorized maker schemes occur when employees with signature authority write fraudulent checks for their own benefit

Item #	Procedure	Yes	No	Comments
1.	Are unused checks stored in a secure container with limited access?			
2.	Are unused checks from accounts that have been closed promptly destroyed?			
3.	Are electronic payments used where possible to limit the number of paper checks issued?			
4.	Are printed and signed checks mailed immediately after signing?			
5.	Are new checks purchased from reputable check vendors?			
6.	Do company checks contain security features to ensure their integrity?			
7.	Has the company notified its bank to not accept checks over a predetermined maximum amount?			
8.	Has the company established positive pay controls with its bank by supplying the bank with a daily list of checks issued and authorized for payment?			
9.	Is the employee who prepares the check prohibited from signing the check?			
10.	Are detailed comparisons made between the payees on the checks and the payees listed in the cash disbursements journal?			
11.	Are employees responsible for handling and coding checks periodically rotated?			

MODULE 6 - Check Tampering Schemes

Check Tampering Schemes Include: 1) forged maker schemes involve forging an authorized signature on a company check, 2) forged endorsements schemes consist of forging the signature endorsement of an intended recipient of a company check, 3) Altered payee schemes involve changing the payee designation on the check to the perpetrator or an accomplice, 4) Authorized maker schemes occur when employees with signature authority write fraudulent checks for their own benefit

Item #	Procedure	Yes	No	Comments
12.	Are bank reconciliations completed immediately after the statements are received?			
13.	Are bank statements and account reconciliations independently audited to confirm accuracy?			
14.	Are cancelled checks independently reviewed for alterations and forgeries?			
15.	Are checks for a material amount matched to the supporting documentation?			
16.	Are voided checks examined for irregularities and to ensure they haven't been processed?			
17.	Are missing checks recorded and stop payments issued?			
18.	Do questionable payees or payee addresses trigger review of the corresponding check and support documentation?			
19.	With the exception of payroll, are checks issued to employees reviewed for irregularities?			
20.	Are two signatures required for check issuance?			
21.	Are all company payments made by check or other recordable payment device?			
22.	Are handwritten checks prohibited?			

MODULE 7 - Cash Register Schemes

False refund schemes occur when an employee 1) issues a refund for fictitious merchandise and keeps the money or, 2) overstates the amount of merchandise returned and skims the excess money. False void schemes occur when a register worker retains a customer receipt, processes a fictitious voided sale, and keeps the money.

Item #	Procedure	Yes	No	Comments
1.	Are refunds, voids, and discounts evaluated on a routine basis to identify patterns of activity among employees, departments, shifts, merchandise, etc.?			
2.	Is there a sign posted at the register asking the customer to request and examine a sales receipt?			
3.	Are cash disbursements recorded on a pre-numbered form and reconciled daily?			
4.	Do the cash disbursement forms have an explanation section or code?			
5.	Are customers that are involved in voided sales and refunds randomly contacted to verify the accuracy of the transaction?			
6.	Is access to the necessary control keys for refunds and voids restricted to supervisors?			
7.	Do void or refund transactions have to be approved by a supervisor and documented?			
8.	Is documentation of void and refund transactions maintained on file?			
9.	Is missing or altered register tape thoroughly investigated?			
10.	Are gaps in the register tape investigated?			
11.	Are multiple voids or refunds for amounts just under any review limit investigated?			

MODULE 7 - Cash Register Schemes

False refund schemes occur when an employee 1) issues a refund for fictitious merchandise and keeps the money or, 2) overstates the amount of merchandise returned and skims the excess money. False void schemes occur when a register worker retains a customer receipt, processes a fictitious voided sale, and keeps the money.

Item #	Procedure	Yes	No	Comments
12.	Is an employee other than the register worker responsible for preparing register count sheets and comparing them to register totals?			
13.	Are customer complaints regarding payment errors thoroughly investigated?			
14.	Does each cashier have a separate access code to the register?			
15.	Does each cashier have a separate cash drawer?			
16.	Is an over and short log kept for each person and/or register?			
17.	Are over and short incidents thoroughly investigated and monitored?			
18.	Are all "no sale" receipts accounted for and attached to a daily cashier's report?			
19.	Is access to the register area restricted to authorized employees and supervisors?			
20.	Are all cashiers periodically integrity shopped?			

MODULE 8 - Purchasing and Billing Schemes

1) Shell company schemes occur when an employee submits invoices for payment from a fictitious company controlled by the employee 2) pay and return schemes occur when an employee arranges for overpayment of a vendor invoice and pockets the overpayment amount when it is returned to the company 3) Personal purchase schemes occur when an employee submits an invoice for personal purchases to the company for payment, or when an employee uses a company credit card for personal use.

Item #	Procedure	Yes	No	Comments
1.	Does the organization have a purchasing department?			
2.	Is the purchasing department independent of the accounting, receiving, and shipping departments?			
3.	Do purchase requisitions require management approval?			
4.	Do purchase orders specify a description of items, quantities, prices, and dates?			
5.	Are purchase order forms pre-numbered and accounted for?			
6.	Does the company maintain a master vendor file?			
7.	Are competitive bids required for all purchases?			
8.	Does the receiving department prepare receiving reports for all items received?			
9.	Does the receiving department maintain a log of all items received?			
10.	Are copies of receiving reports furnished to the accounting and purchasing departments?			
11.	Are purchasing and receiving functions separate from invoice processing, accounts payable, and general ledger functions?			
12.	Are vendor invoices, receiving reports, and purchase orders matched before the related liability is recorded?			

MODULE 8 - Purchasing and Billing Schemes

1) Shell company schemes occur when an employee submits invoices for payment from a fictitious company controlled by the employee 2) pay and return schemes occur when an employee arranges for overpayment of a vendor invoice and pockets the overpayment amount when it is returned to the company 3) Personal purchase schemes occur when an employee submits an invoice for personal purchases to the company for payment, or when an employee uses a company credit card for personal use.

Item #	Procedure	Yes	No	Comments
13.	Are purchase orders recorded in a purchase register or voucher register before being processed through cash disbursements?			
14.	Are procedures adequate to ensure that merchandise purchased for direct delivery to the customer is promptly billed to the customer and recorded as both a receivable and a payable?			
15.	Are records of goods returned to vendors matched to vendor credit memos?			
16.	Is the accounts payable ledger or voucher register reconciled monthly to the general ledger control accounts?			
17.	Do write-offs of accounts payable debit balances require approval of a designated manager?			
18.	Is the master vendor file periodically reviewed for unusual vendors and addresses?			
19.	Are vendor purchases analyzed for abnormal levels?			
20.	Are control methods in place to check for duplicate invoices and purchase order numbers?			
21.	Are credit card statements reviewed monthly for irregularities?			
22.	Are vendors with post office box addresses verified?			
23.	Are voucher payments reviewed regularly for proper documentation?			

MODULE 8 - Purchasing and Billing Schemes

1) Shell company schemes occur when an employee submits invoices for payment from a fictitious company controlled by the employee 2) pay and return schemes occur when an employee arranges for overpayment of a vendor invoice and pockets the overpayment amount when it is returned to the company 3) Personal purchase schemes occur when an employee submits an invoice for personal purchases to the company for payment, or when an employee uses a company credit card for personal use.

Item #	Procedure	Yes	No	Comments
24.	Is access to the accounts payable subledger and the general ledger restricted? Does access create an audit trail?			

MODULE 9 - Payroll Schemes

1) Ghost employee schemes occur when a person not employed by the company is on the payroll. 2) Overpayment schemes occur when a company pays an employee based on falsified hours or rates. 3) Commission schemes occur when the amount of sales made or the rate of commission is fraudulently inflated.

Item #	Procedure	Yes	No	Comments
1.	Is the employee payroll list reviewed periodically for duplicate or missing social security numbers?			
2.	Are personnel records maintained independently of payroll and timekeeping functions?			
3.	Are references checked on all new hires?			
4.	Are sick leave, vacations, and holidays reviewed for compliance with company policy?			
5.	Are appropriate forms completed and signed by the employee to authorize payroll deductions and withholding exemptions?			
6.	Is payroll periodically compared with personnel records for terminations?			
7.	Are payroll checks pre-numbered and issued in sequential order?			
8.	Is the payroll bank account reconciled by an employee who is not involved in preparing payroll checks, does not sign the checks, and does not handle payroll distribution?			
9.	Are payroll registers reconciled to general ledger control accounts?			
10.	Are cancelled payroll checks examined for alterations and endorsements?			
11.	Is access restricted to payroll check stock and signature stamps?			

MODULE 9 - Payroll Schemes

1) Ghost employee schemes occur when a person not employed by the company is on the payroll. 2) Overpayment schemes occur when a company pays an employee based on falsified hours or rates. 3) Commission schemes occur when the amount of sales made or the rate of commission is fraudulently inflated.

Item #	Procedure	Yes	No	Comments
12.	Are payroll withholdings for taxes, insurance, etc. examined to determine if any employees are not having these items deducted from their paychecks?			
13.	Is the employee payroll list reviewed periodically for duplicate or missing home addresses and telephone numbers?			
14.	Is the account information for automatically deposited payroll checks reviewed periodically for duplicate entries?			
15.	Is an employee separate from the payroll department assigned to distribute payroll checks?			
16.	Are new employees required to furnish proof of immigration status?			
17.	Does any change to an employee's salary require more than one level of management approval?			
18.	Does overtime have to be authorized by a supervisor?			
19.	Do supervisors verify and sign timecards for each pay period?			
20.	Are commission expenses compared to sales figures to verify amounts?			
21.	Does someone separate from the sales department calculate sales commissions?			

MODULE 10 - Expense Schemes

1) Mischaracterized expense schemes occur when an employee requests reimbursement for a personal expense, claiming the expense to be business related. 2) Overstated expense schemes occur when an employee overstates the cost of actual expenses and seeks reimbursement. 3) Fictitious expense schemes occur when an employee invents a purchase and seeks reimbursement for it. 4) Multiple reimbursement schemes occur when an employee submits a single expense for reimbursement multiple times.

Item #	Procedure	Yes	No	Comments
1.	Are the expense accounts reviewed and analyzed periodically using historical comparisons or comparisons with budgeted amounts?			
2.	Do employee expense reimbursement claims receive a detailed review before payment is made?			
3.	Are employees required to submit detailed expense reports?			
4.	Is a limit placed on expenses such as hotels, meals, and entertainment?			
5.	Are receipts required for all expenses to be reimbursed?			
6.	Are supervisors required to review and approve all expense reimbursement requests?			
7.	Is there a random authentication of expense receipts and expenses claimed?			

MODULE 11 - Theft of Inventory and Equipment

1) Fake sale schemes occur when an accomplice of an employee "buys" merchandise, but the employee does not ring up the sale and the accomplice takes the merchandise without making any payment, 2) Purchasing schemes occur when an employee with purchasing authority uses that authority to purchase and misappropriate merchandise, 3) Receiving schemes occur when an employee misappropriates assets purchased by the company as they are received at the company, 4) False shipment schemes occur when an employee creates false sales documents and false shipping documents to make it appear that missing inventory was not actually stolen, but rather sold, 5) Misuse of company assets occurs when an employee borrows company assets for personal use without authorization, 6) Larceny schemes occur when an employee takes inventory from the company premises without attempting to conceal the theft in the accounting records.

Item #	Procedure	Yes	No	Comments
1.	Has a recent inventory of company equipment, listing serial numbers and descriptions, been completed?			
2.	Does the company assign an individual from outside of the department to conduct the department's inventory?			
3.	Are unexplained entries to the inventory records examined for source documentation?			
4.	Is the company experiencing sizeable inventory increases without comparable sales increases?			
5.	Are analytical reviews of beginning inventory, sales, cost of goods sold, and ending inventory conducted periodically to look for unexplained differences?			
6.	Is there an unusual volume of inventory adjustments, write-offs, or disposals?			
7.	Does the organization have written inventory instructions and orders?			
8.	Does someone independent of the purchasing, receiving, and warehousing functions physically count the inventory?			
9.	Are pre-numbered inventory tags used?			
10.	Are the inventory tags controlled and accounted for?			

MODULE 11 - Theft of Inventory and Equipment

1) Fake sale schemes occur when an accomplice of an employee "buys" merchandise, but the employee does not ring up the sale and the accomplice takes the merchandise without making any payment, 2) Purchasing schemes occur when an employee with purchasing authority uses that authority to purchase and misappropriate merchandise, 3) Receiving schemes occur when an employee misappropriates assets purchased by the company as they are received at the company, 4) False shipment schemes occur when an employee creates false sales documents and false shipping documents to make it appear that missing inventory was not actually stolen, but rather sold, 5) Misuse of company assets occurs when an employee borrows company assets for personal use without authorization, 6) Larceny schemes occur when an employee takes inventory from the company premises without attempting to conceal the theft in the accounting records.

Item #	Procedure	Yes	No	Comments
11.	Do the inventory procedures prevent double counting?			
12.	Are inventory counts subject to independent recounts?			
13.	Is the inventory reasonably identifiable for proper classification in the accounting system, such as description, condition, or stage of completion?			
14.	Are differences between physical counts and inventory records investigated before inventory records are adjusted?			
15.	Is scrap inventoried and is scrap disposal accounted for?			
16.	Are the following duties segregated: Requisition of inventory, receiving of inventory, disbursement of inventory, writing off of inventory as scrap, and receipt of proceeds from the sale of scrap inventory.			
17.	Is a receiving report prepared for all purchased goods?			
18.	Are copies of receiving reports sent directly to the purchasing and accounting departments?			
19.	Is the receiving department provided with a copy of the purchase order on all items to be received?			
20.	Are partial shipments annotated on purchase orders or attached as separate sheets?			

MODULE 11 - Theft of Inventory and Equipment

1) Fake sale schemes occur when an accomplice of an employee "buys" merchandise, but the employee does not ring up the sale and the accomplice takes the merchandise without making any payment, 2) Purchasing schemes occur when an employee with purchasing authority uses that authority to purchase and misappropriate merchandise, 3) Receiving schemes occur when an employee misappropriates assets purchased by the company as they are received at the company, 4) False shipment schemes occur when an employee creates false sales documents and false shipping documents to make it appear that missing inventory was not actually stolen, but rather sold, 5) Misuse of company assets occurs when an employee borrows company assets for personal use without authorization, 6) Larceny schemes occur when an employee takes inventory from the company premises without attempting to conceal the theft in the accounting records.

Item #	Procedure	Yes	No	Comments
21.	Are overage, shortage, and damage reports completed and sent to the purchasing and accounting departments?			
22.	Are quantities of materials received counted and compared to purchase orders?			
23.	Is there a written policy allowing management to inspect all desks, file cabinets, and other containers on company property?			
24.	Is there an equipment removal authorization policy requiring written management approval to remove any company equipment from the company premises?			
25.	Is there a policy requiring the inspection of packages, boxes, and other containers before they leave the company premises?			
26.	Is the removal of trash and trash receptacles periodically monitored?			
27.	Are the shipping and receiving areas adequately supervised to prevent theft?			
28.	Are high volume items stored in secure or continuously monitored areas?			
29.	Is the shipping function separate from the purchasing and inventory functions?			
30.	Are shipping documents pre-numbered and accounted for?			

MODULE 11 - Theft of Inventory and Equipment

1) Fake sale schemes occur when an accomplice of an employee "buys" merchandise, but the employee does not ring up the sale and the accomplice takes the merchandise without making any payment, 2) Purchasing schemes occur when an employee with purchasing authority uses that authority to purchase and misappropriate merchandise, 3) Receiving schemes occur when an employee misappropriates assets purchased by the company as they are received at the company, 4) False shipment schemes occur when an employee creates false sales documents and false shipping documents to make it appear that missing inventory was not actually stolen, but rather sold, 5) Misuse of company assets occurs when an employee borrows company assets for personal use without authorization, 6) Larceny schemes occur when an employee takes inventory from the company premises without attempting to conceal the theft in the accounting records.

Item #	Procedure	Yes	No	Comments
31.	Are shipping orders matched with sales orders and contracts?			
32.	Are shipments of goods required to have authorized sales orders and contracts prior to shipping?			
33.	Are shipping documents forwarded directly to the accounting department for recording inventory reduction and cost of sales?			

MODULE 12 - Theft of Proprietary Information

Theft of proprietary information involves theft or disclosure of confidential or trade secret information for financial gain.

Item #	Procedure	Yes	No	Comments
1.	Are there policies and procedures addressing the identification, classification, and handling of proprietary information?			
2.	Are employees who have access to proprietary information required to sign nondisclosure agreements?			
3.	Are employees who have access to proprietary information required to sign noncompete agreements to prevent them from working for competitors within a stated period of time and location?			
4.	Are employees provided with training to make them aware of proprietary information, their responsibility to protect the information, and the company policies and procedures relating to proprietary information?			
5.	Is there an established procedure to identify what information should be classified as sensitive and for how long?			
6.	Are sensitive documents properly classified and marked as confidential?			
7.	Is sensitive information properly secured when not being used?			
8.	Is access to sensitive information physically controlled and accounted for?			
9.	Is sensitive information promptly destroyed when it is no longer needed?			
10.	Are compromises to the security of proprietary information promptly investigated to determine the source?			
11.	Are employees required to use screensaver and/or server passwords to protect unattended computer systems?			

MODULE 12 - Theft of Proprietary Information

Theft of proprietary information involves theft or disclosure of confidential or trade secret information for financial gain.

Item #	Procedure	Yes	No	Comments
12.	Are confidential documents shredded when discarded?			

MODULE 13 - Corruption

1) Bribery schemes involve the offering, giving, receiving, or soliciting of a thing of value to influence a business decision
 2) Kickback schemes occur when vendors make undisclosed payments to employees of purchasing companies in order to enlist the employees in overbilling schemes. 3) Bid-rigging schemes occur when an employee fraudulently assists a vendor in winning a contract through the competitive bidding process. 4) Economic extortion schemes occur when an employee demands payment from a vendor decisions made in the vendor's favor. Refusal to pay the extortion results in harm to the vendor. 5) Illegal gratuities schemes involve giving or receiving something of value to reward a business decision.

Item #	Procedure	Yes	No	Comments
1.	Is there a company policy that addresses the receipt of gifts, discounts, and services offered by a supplier or customer?			
2.	Is there an established bidding policy?			
3.	Are purchases reviewed to detect out of line costs?			
4.	Are purchases reviewed to identify favored vendors?			
5.	Are purchases reviewed to identify excessive amounts?			
6.	Are pre-bid solicitation documents reviewed for any restrictions on competition?			
7.	Are bid solicitation packages numbered and controlled?			
8.	Is communication between bidders and purchasing employees restricted?			
9.	Are the bids received kept confidential?			
10.	Are bidder's qualifications verified?			
11.	Are contracts awarded based on predetermined criteria?			
12.	Are purchasing account assignments rotated?			
13.	Are vendors surveyed periodically regarding company purchasing practices?			

MODULE 14 - Conflicts of Interest

1) Purchase schemes involve the overbilling of a company for goods or services by a vendor in which an employee has an undisclosed ownership or financial interest. 2) Sales schemes involve the underselling of company goods by an employee to a company in which the employee maintains a hidden interest.

Item #	Procedure	Yes	No	Comments
1.	Are there periodic comparisons of vendor information with employee information, such as addresses and telephone numbers?			
2.	Are vendors who employ former company employees under increased scrutiny?			
3.	Does the organization have a reporting procedure for personnel to report their concerns about vendors receiving favored treatment?			
4.	Are employees required to complete an annual disclosure document that includes business ownership, income, and investment information?			
5.	Does the organization require vendors to sign an agreement allowing vendor audits?			
6.	Are vendor audits conducted by someone independent of the purchase, sales, billing, and receiving departments?			

MODULE 15 - Fraudulent Financial Reports

1) Fictitious revenue schemes involve recording fictitious revenue from the sale of goods or services. 2) Improper timing schemes involve recording revenues or expenses in improper accounting periods. 3) Understating liabilities schemes involve concealing or understating liabilities and expenses, capitalizing expenses, or expensing capital expenses. 4) Improper disclosure schemes involve the improper disclosure of material information, such as contingent liabilities, significant events, management fraud, related party transactions, or accounting changes. 5) Improper asset valuation schemes involve the improper valuation of inventory, accounts receivable, fixed assets, intangibles, or other assets.

Item #	Procedure	Yes	No	Comments
1.	Are the organization's accounting records in proper form?			
2.	Does the organization employ an adequate number of accounting employees?			
3.	Does the organization have an effective internal audit staff?			
4.	Are proper internal controls established and maintained?			
5.	Does the organization embrace the concept of internal controls?			
6.	Are senior managers visible in their support of internal controls?			
7.	Are the organization's financial goals and objectives realistic?			
8.	Does the organization consistently achieve its financial goals and objectives?			
9.	Is the organization's reported financial performance stable or increasing?			
10.	Does the company have stable relationships with its banks?			
11.	Are there unrealistic changes or increases in financial statement account balances?			
12.	Are the account balances realistic given the nature, age, and size of the company?			

MODULE 15 - Fraudulent Financial Reports

1) Fictitious revenue schemes involve recording fictitious revenue from the sale of goods or services. 2) Improper timing schemes involve recording revenues or expenses in improper accounting periods. 3) Understating liabilities schemes involve concealing or understating liabilities and expenses, capitalizing expenses, or expensing capital expenses. 4) Improper disclosure schemes involve the improper disclosure of material information, such as contingent liabilities, significant events, management fraud, related party transactions, or accounting changes. 5) Improper asset valuation schemes involve the improper valuation of inventory, accounts receivable, fixed assets, intangibles, or other assets.

Item #	Procedure	Yes	No	Comments
13.	Do actual physical assets exist in the amounts and values indicated on the financial statements?			
14.	Have there been significant changes in the nature of the organization's revenues and expenses?			
15.	Do one or a few large transactions account for a significant portion of any account balance or amount?			
16.	Are there significant transactions that occur near the end of a period that positively impact results of operations, especially transactions that are unusual or highly complex?			
17.	Are financial results fairly consistent across periods?			
18.	Is there an inability to generate cash flows from operations while experiencing earnings growth?			
19.	Is there significant pressure to obtain additional capital necessary to stay competitive?			
20.	Are reported assets, liabilities, revenues, or expenses based on significant estimates that involve unusually subjective judgments or uncertainties?			
21.	Are reported assets, liabilities, revenues, or expenses based on significant estimates that are subject to potential significant change in the near term in a manner that may have a financially disruptive effect on the organization?			

MODULE 15 - Fraudulent Financial Reports

1) Fictitious revenue schemes involve recording fictitious revenue from the sale of goods or services. 2) Improper timing schemes involve recording revenues or expenses in improper accounting periods. 3) Understating liabilities schemes involve concealing or understating liabilities and expenses, capitalizing expenses, or expensing capital expenses. 4) Improper disclosure schemes involve the improper disclosure of material information, such as contingent liabilities, significant events, management fraud, related party transactions, or accounting changes. 5) Improper asset valuation schemes involve the improper valuation of inventory, accounts receivable, fixed assets, intangibles, or other assets.

Item #	Procedure	Yes	No	Comments
22.	Is the company experiencing unusually rapid growth or profitability, especially when compared with that of other companies in the same industry?			
23.	Is the organization highly vulnerable to changes in interest rates?			
24.	Are there unrealistically aggressive sales or profitability incentive programs?			
25.	Is there a threat of imminent bankruptcy, foreclosure, or hostile takeover?			
26.	Is there a high possibility of adverse consequences on significant pending transactions, such as business combinations or contract awards, if poor financial results are reported?			
27.	Is there a poor or deteriorating financial position when management has personally guaranteed significant debts of the entity?			
28.	Does the company continuously operate on a crisis basis or without a careful budgeting and planning process?			
29.	Does the organization have difficulty collecting receivables or have other cash flow problems?			
30.	Is the organization dependent on one or two key products or services, especially products or services that can become quickly obsolete?			
31.	Do the footnotes contain information about complex issues?			
32.	Are there adequate disclosures in the financials and footnotes?			

EXHIBIT F2

Fraud Risk Assessment Framework

FRAUD RISK ASSESSMENT FRAMEWORK			
Identified Fraud Risks and Schemes	Likelihood	Financial Significance	Risk Ref. No.
<i>Misappropriation of Assets:</i>			
<i>Corruption:</i>			
<i>Financial Statement Fraud:</i>			

EXHIBIT G1

Sample Control Activities Documentation Form

COMPANY NAME**Anti-fraud Program****Documentation of Control Activities****Dated:****Control Activities***New Vendor Establishment Procedures*

1	A Master Vendor File will be maintained and updated on a regular basis
2	A New Vendor Establishment Form will be initiated within the accounts payable department for all new vendors
3	Information to be obtained for the form will be requested from the new vendor and completed by Accounts Payable Clerk #1
4	Accounts Payable Clerk #1 will forward the information completed portion of the New Vendor Establishment form to Accounts Payable Clerk #2
5	Accounts Payable Clerk #2 will then validate the information on the form. Validation and verification will include: Phone calls to numbers provided Test email message to the email provided Web based search engine inquiries State tax base searches Online mapping or Google Earth searches of address provided
6	Accounts Payable Clerk #2 will forward the completed New Vendor Establishment Form to Management for approval
7	The approved New Vendor Establishment form, along with any other documentation from the vendor, will be added to the Master Vendor File
8	As a part of the formal monitoring program, compliance with the review of the supporting documentation and form completion for the Master Vendor File will be audited annually to determine the level of adherence to that control activity.

EXHIBIT H1

Establishing an Effective Anti-Fraud Training Program



Designing an Effective Anti-Fraud Training Program

By implementing an effective fraud awareness program, management can harness the efforts of the full staff in its anti-fraud activities and can significantly reduce the cost of fraud within the organization. The following are important considerations that must be addressed when designing an employee anti-fraud training program to ensure its effectiveness.

Who Should Attend?

Every employee within the organization should be mandated to participate in the fraud awareness training program. No individuals — regardless of their position within the organization — should be provided an exemption from receiving an initial orientation and ongoing anti-fraud education.

Targeted Training for Managers and Executives

In addition to the information presented to all employees, managers and executives should receive special training that addresses the added fraud prevention and detection responsibility — and ability — provided by their positions of authority. For example, department managers should be trained in the specific warning signs and prevention/detection methods pertinent to their department's functions. Purchasing managers should be well versed in the red flags of bribery schemes; likewise, controllers should understand just how important their vigilance is in preventing and detecting fraudulent disbursements.

Frequency and Length of Fraud Awareness Training

Like any educational efforts, frequent exposure to anti-fraud topics is the key to ensuring employees absorb — and apply — the information provided. Formal fraud awareness training should be an ongoing process that begins at the time of hire. Employees should also participate in refresher training at least annually to help keep the program alive and ingrained in their minds. Additionally, all employees should sign an annual statement acknowledging their understanding of and commitment to the program.



Training Delivery Methods

Formal anti-fraud training can take many forms, including live, in-class instruction; recorded video or animated courses; or interactive self-study programs. Of these options, a live class is preferable, as it allows employees the opportunity to actively participate, interact with other employees, discuss the true fraud risks facing the organization, and seek and provide feedback regarding the anti-fraud program as a whole. Integrating games

and role-playing exercises into the training curriculum can make the course more enjoyable — and thus more effective — for participants. Perhaps most important, however, is that the training be based on the realities of the organization, rather than on generic anti-fraud messages. While providing general information is good and necessary, doing so without addressing the specific concerns of the company or providing employees with practical knowledge and ideas on how to apply it will render the training program ineffective.



Designing an Effective Anti-Fraud Training Program

In addition, the organization can use other informal means to reinforce its anti-fraud stance on a more constant basis. Periodic newsletters, posters in break rooms, and other casual reminders help keep fraud prevention and detection in the front of employees' minds.

Topics to Cover

The following topics should form the basis of the training, but the information presented should focus on the specific risks faced by the organization in order to provide employees with practical, implementable knowledge.

What Fraud Is and What It Is Not

A good anti-fraud training program informs employees of what behavior is acceptable and what is not. Providing employees with the legal definition of fraud is not enough; effective training includes an interactive discussion and examples of fraud, as well as examples of errors and abuse.

How Fraud Hurts the Organization

Surprisingly, some employees view the theft of a few thousand dollars from a big organization as having a negligible impact on the company as a whole. Others might believe that fudging numbers in the accounting records to enable the company reach its goals is actually a helpful act.



Fraud awareness training programs must make clear to employees how such actions harm the organization — how all frauds result in lost resources; decreased productivity; lowered morale; investments of time and money into investigation, punishment, and remediation; and a hit to the company's reputation.

How Fraud Hurts Employees

Employees must also be made aware of how a fraud perpetrated by another individual can negatively affect them personally through decreased salaries, loss of bonuses, possible layoffs, increased scrutiny, decreased trust throughout the organization, and the need to clean up after any mess created. Personalizing the fallout in this way helps increase employees' commitment to aiding fraud prevention and detection efforts.

Who Perpetrates Fraud

The fraud-triangle theory indicates that anyone who has the combination of sufficient pressure, adequate opportunity, and an ability to rationalize a dishonest act is at risk of committing fraud. Fraudsters come in all age groups, income levels, and from both genders. Further, ACFE research shows that the typical fraudster is college educated and does not have a criminal history. Anti-fraud training should work to dispel any preconceived notions held by employees regarding what a fraud perpetrator looks like, and help employees learn to focus on identifying the warning signs of fraudulent behavior.



Designing an Effective Anti-Fraud Training Program

How to Identify Fraud

Instructing employees that they must help the organization fight fraud does little good without some accompanying information about what to look for. The following are some warning signs of fraud that employees should be aware of:

Financial/Transactional Red Flags

- Red flags regarding the structure of or personnel involved in a transaction
- Red flags within the organization's operations
- Red flags within the accounting system
- Red flags regarding the organization's financial performance

Behavioral Red Flags

- Living beyond their means
- Financial difficulties
- Control issues, unwilling to share duties
- Unusually close relationship with vendor/customer
- Wheeler/dealer attitude
- Divorce/family problems
- Irritability, suspiciousness, defensiveness
- Addiction problems
- Unwilling to take vacation days
- Past employment-related problems
- Complained about inadequate pay
- Excessive pressure from within the organization
- Past legal problems
- Instability in life circumstances
- Excessive family/peer pressure for success
- Complained about lack of authority

How to Report Fraud

More fraud is uncovered by tips than by any other means, making employees the best possible fraud detection control. But for employees to be able to serve this function, they must be well informed on how to report any suspicious activity, as well as empowered to make such reports without risk of retribution.

The Punishment for Dishonest Acts

The opportunity to commit fraud becomes more attractive when employees believe fraud normally goes undetected and unprosecuted. Consequently, the punishment (termination and possible prosecution) should be spelled out explicitly to all employees in advance. Providing examples of past transgressions that have been punished can reinforce the stance that such acts will be addressed with certainty, swiftness, and severity.

About the Association of Certified Fraud Examiners

The ACFE is the world's largest anti-fraud organization and premier provider of anti-fraud training and education. Together with nearly 80,000 members in more than 160 countries, the ACFE is reducing business fraud worldwide and leading the fight against white collar crime. For more information about the ACFE, visit ACFE.com.



ACFE.com • info@ACFE.com • (800) 245-3321 • +1 (512) 478-9000

© 2016 Association of Certified Fraud Examiners, Inc. "ACFE," "CFE," "Certified Fraud Examiner," "Association of Certified Fraud Examiners," the ACFE Logo and related trademarks, names and logos are the property of the Association of Certified Fraud Examiners, Inc., and are registered and/or used in the U.S. and countries around the world.

EXHIBIT I1

Sample Compliance Audit Program

COMPLIANCE AUDIT PROGRAM
Control Activity: Authorized Check Signer Approval

Item #	Procedure	Perf. By	Date	Comments
1.	Obtain a list of disbursements for the current month.			
2.	Select twenty disbursements from this list for compliance review.			
3.	Obtain the supporting documentation for each of the selected disbursements.			
4.	Determine the following for each of the selected disbursements: a) Check amount agrees to supporting documentation b) Documentation supports a valid business purpose c) Supporting documentation has been "initialed" by authorized check signer			

Response:

Were exceptions noted? _____

If yes, document the response to these exceptions below:

Signature: _____

Date: _____

Title: _____

EXHIBIT I2

Sample Compliance Audit Workpaper

Company Name

Compliance Testing

Performed by: _____

Control Activity: Authorized Check Signer Approval

Month Tested: _____

Disb #	Date	Amount	Payee	Support Doc.	1	2	3	Exceptions
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
16								
17								
18								
19								
20								

Attributes Tested:

- 1 Check amount agrees to supporting documentation
- 2 Documentation supports a valid business purpose
- 3 Supporting documentation has been "initialed" by authorized check signer

EXHIBIT I3

Sample Anti-Fraud Report

JEMEZ MOUNTAINS ELECTRIC COOPERATIVE

Internal Audit / Anti-Fraud Program Monthly Report

Month: August 20XX

Areas Addressed

Fraud Risk Assessment

Along with the fraud risk assessment team, we addressed internal controls associated with the warehouse / inventory control. Vulnerabilities of fraud risk identified are included on the attached Fraud Risk Assessment Framework.

Control Activities

In response to the risks identified in the Fraud Risk Assessment, the control activities development team designed and implemented the internal controls included on the attached Control Activities Form.

Anti-Fraud / Fraud Awareness Training

This month, we addressed fraud trends in our industry as a part of the Cooperative-wide staff meeting conducted on _____.

Monitoring / Routine Maintenance

As documented in our workpapers, not provided herein, we conducted a compliance audit of the approval process for disbursements, the establishment of new vendors, and authorized check signers for checks.

Those audits resulted in the identification of noncompliance as follows:

Based on these instances of noncompliance, we retrained the applicable employee regarding the operation of the internal controls [or conversely, we redesigned the internal control] as follows:

Signature and Title

Date