How Local Agencies Can Better Manage Their Treasury Risk

Ben Leavitt, CPA, CFE
John Dominguez, CPA, CFE, CGMA
Our Session Today

* Defining Risk
* Key Elements in a Sound Internal Control Structure
* Risks in Treasury Operations
* Is Fraud occurring within your organization? What Can Go Wrong and Prevention Tips
DEFINING RISK
What is Risk?

* In general business – risk = potential for loss
  * From error, fraud, inefficiency, failure to comply, reputation damage, litigation, etc.
* In auditing - potential for risk of material misstatement or noncompliance
* Risk assessment is a process to evaluate risk
* Why should an organization assess risk?
  * Focuses attention on areas most significant and susceptible to error or fraud
  * Allocates limited treasury resources
  * Prioritizes decisions on system improvements/upgrades, frequency and timing of control activities, internal audit plans and monitoring procedures
In response, the AICPA released the improved guidance related to fraud and new risk assessment standards

2002: SAS 99, *Consideration of Fraud in a Financial Statement Audit*, supercedes SAS 82. Key topics:

- The importance of professional skepticism
- Two types of effects that fraud can have on financial statements:
  - Misstatements due to fraudulent financial report (FFR)
  - Misstatements due to misappropriation of assets (MA)
- Introduction to fraud triangle (fraud risk factors)
  - Incentives and pressures
  - Opportunity
  - Rationalizations and attitude
- Emphasis on Management’s ability to perpetrate or cover up fraud
- Introduction of fraud brainstorming session by audit engagement team
The evolution of “Fraud Triangle”

- Originally fraud triangle (fraud risk factors)
  - Incentives and pressures
  - Opportunity
  - Rationalizations and attitude
- Evolved into fraud diamond
  - Motive, Pressure, Incentive
  - Opportunity
  - Rationalization
- **CAPABILITY**
  - Position/Function
  - Intellect
  - Confidence/Ego
  - Coercion skills
  - Immunity to stress
KEY ELEMENTS IN A SOUND ORGANIZATIONAL CONTROL STRUCTURE
Process, effected by board, management, and others to provide reasonable assurance regarding:
* Effectiveness and efficiency of operations
* Reliability of financial reporting
* Compliance with applicable laws and regulations
COSO Definition: 5 Interrelated Internal Control Components

* COSO: Committee of Sponsoring Organizations of the Treadway Commission (formed 1985)
  * Control Environment
  * Risk Assessment
  * Control Activities
  * Information and Communication
  * Monitoring
Control Environment

* Tone of the organization
* Integrity, ethical values, and competence of an organization’s people
* Management’s philosophy and operating style
* Management’s assignment of authority and responsibility
* Approach to developing people
* Attention and direction provided by the board
Risk Assessment

* Precondition: establish objectives, linked at different levels and internally consistent
* Identification and analysis of relevant risks to the achievement of objectives
* Mechanisms are needed to identify and deal with special risks associated with change
Risk Assessment
Policies and procedures to help ensure management directives are carried out

* Ensure necessary actions are taken to address risks
* Occur throughout organization, at all levels and functions
* Activities may include: approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties
Control Activities
Information systems produce reports containing financial, operational, and compliance-related information, making it possible to run and control the organization.

Effective communication must occur, flowing down, across, and up the organization.

Personnel must have a clear message from management that control activities must be taken seriously.

Communication with external parties: customers/community, suppliers, regulators.
- Process that assesses the quality of the system’s performance over time
- Ongoing monitoring activities: regular management and supervisory activities, and other actions personnel take in performing their duties
- Separate evaluations: scope and frequency depends on risk assessment and effectiveness of ongoing monitoring
- Deficiencies in internal control should be reported upstream, with significant matters to top management and the board
Monitoring procedures (COSO guidance on monitoring internal control systems):

- Periodic evaluation and testing of controls by internal audit
- Continuous monitoring built into information systems
- Analysis of, and appropriate follow-up on, operating reports that might identify control failures
- Supervisory reviews of controls, such as reconciliation reviews, as part of normal process
- Self-assessments by board and management of tone
- Audit committee inquiries of internal/external auditors
- Quality assurance reviews of the internal audit dept.
Monitoring
Roles and Responsibilities

* Board of Supervisors/Directors: provides governance, guidance, and oversight
* Management: County Treasurer is ultimately responsible and should assume “ownership” of the system
* Financial officers and their staffs: control activities cut across, as well as up and down, the operating and other units of an enterprise
* IT officer: control over information safeguarding, compliance, authorization, accuracy, backup & recovery of information
* Internal Auditors: provide monitoring function, evaluating effectiveness of control systems
Other Personnel

* Internal control is, to some degree, the responsibility of everyone in an organization
* Production of information used in the internal control system or take other actions needed to effect control
* Responsibility for communicating upward problems in operations, noncompliance with code of conduct, or other policy violations or illegal actions
* External auditors provide an independent and objective view – providing information useful to management and the board
  * External parties such as external auditors, legislators, regulators, news media, etc. are not responsible for and are not a part of an organization’s internal control system
RISKS IN TREASURY OPERATIONS
2012 REPORT TO THE NATIONS

* Online 85-question survey of 34,275 CFEs
* Oct-Dec 2011
* 1,388 responses (CWDL partners contributed with a case included in the 2012 study)
2012 REPORT TO THE NATIONS

Industry of Victim Organizations

- Banking and Financial Services: 16.7% (2012), 16.6% (2010)
- Government and Public Administration: 10.3% (2012), 9.6% (2010)
- Manufacturing: 10.1% (2012), 10.7% (2010)
- Health Care: 6.7% (2012), 5.9% (2010)
- Education: 5.6% (2012), 6.4% (2010)
- Retail: 6.1% (2012), 6.6% (2010)
- Insurance: 5.7% (2012), 6.0% (2010)
- Services (Professional): 4.0% (2012), 4.0% (2010)
- Religious, Charitable or Social Services: 3.4% (2012), 3.3% (2010)
- Services (Other): 3.5% (2012), 4.0% (2010)
- Construction: 3.4% (2012), 4.9% (2010)
- Oil and Gas: 3.2% (2012), 4.3% (2010)
- Telecommunications: 3.1% (2012), 2.1% (2010)
- Technology: 2.8% (2012), 2.6% (2010)
- Transportation and Warehousing: 3.6% (2012), 3.4% (2010)
- Arts, Entertainment and Recreation: 2.3% (2012), 2.7% (2010)
- Real Estate: 2.0% (2012), 3.2% (2010)
- Wholesale Trade: 2.0% (2012), 2.3% (2010)
- Utilities: 1.9% (2012), 2.6% (2010)
- Agriculture, Forestry, Fishing and Hunting: 1.5% (2012), 1.5% (2010)
- Mining: 0.7% (2012), 0.7% (2010)
- Communications and Publishing: 0.7% (2012), 0.6% (2010)
- Other*: 0.5% (2012), 0.6% (2010)

*Other* category was not included in the 2010 Report.
2012 REPORT TO THE NATIONS

Education of Perpetrator — Frequency

- Postgraduate Degree: 16.9% (2012), 14.0% (2010), 10.9% (2008)
- College Degree: 36.9% (2012), 38.0% (2010), 34.4% (2008)
- Some College: 20.5% (2012), 17.1% (2010), 20.8% (2008)
- High School Graduate or Less: 25.3% (2012), 28.8% (2010), 33.9% (2008)
- Other*: 0.5%

*Other* category was not included in the prior years' reports.
2012 REPORT TO THE NATIONS
2012 REPORT TO THE NATIONS

Perpetrator’s Criminal Background

- Never Charged or Convicted: 87.3% (2012), 85.7% (2010), 87.4% (2008)
- Had Prior Convictions: 5.6% (2012), 6.7% (2010), 6.8% (2008)
- Charged But Not Convicted: 5.9% (2012), 7.7% (2010), 5.7% (2008)
- Other*: 1.2% (2012)

**Note:** *Other* category was not included in the prior years' reports.
* Participant registration & wire request procedures
* Reconciliations – bank, investment inventory, g/l
* Compliance with investment policies and Government Code
* Unclaimed monies distribution controls
* Association with financial institutions
* Potential for management override of controls
IS FRAUD OCCURRING WITHIN YOUR ORGANIZATION? WHAT CAN GO WRONG AND PREVENTION TIPS
Beaufort County Treasurer’s Office employee pleads guilty in embezzlement scheme

- Scheme spanned over 2.5 years
- Created fictitious vendor accounts
- Issued fraudulent over-payment refunds
- Deposited into personal accounts
- Employee was caught, quit, then re-hired less than 12 months later
- Embezzled over $200,000

Internal Control Meltdowns
2012 – Owner of Onyx Capital Advisors indicted for embezzling more than $3 million from three public pension funds.

* Bribing and providing kickbacks to public officials in position of influence
* Received $30 million in pension funds, the three funds suffered losses of $23.8 million
* $8 million of pension funds used to pay for construction of new home in Atlanta
2012 – Former Detroit, MI City Treasurer indicted for accepting

- Cash, gambling money
- Golf clubs
- Tickets to Las Vegas shows
- Massages
- Limousine rides, free flights

In return for approving more than $200M in pension fund investments – resulting investment losses cost the pension funds $84M.
2012 – St. Louis, MO city parking contractor pled guilty to defrauding the Treasurer’s Office.

Firm set up two ghost employees between 6/2009-12/2011, billing for $328K for work that was never performed.
2010 – Malden, MA City Treasurer resigned after treasury department employee pleaded guilty to embezzling $500,000 from the city

26yr old employee issued property tax overpayment refunds to accomplice payees
1990s– Mass. State Treasury defrauded in numerous instances:

* Attempted $6.5M theft from unpaid check fund (collusion with UCF accountant)
* $1.6M theft from unpaid check fund (collusion with Deputy Treasurer & UCF accountant)
* $60,000 cash theft from Treasury vault (Treasury cash management employee – funds not properly recorded)

Culture of Treasury under State Treasurer “secure as a 10-year old’s piggy bank.”
Focus is on “control activities” to prevent asset misappropriation or fraudulent financial reporting, such as:

- **Segregation of duties**: no one person or department should be in a position to initiate, record, and execute a transaction (access to assets and ability to cover up)
- **Physical controls**: limit access and provide security
- **Reconciliation**: independent comparisons
- **Supervision and review**: oversight controls including independent reviews and budget monitoring
- **IT controls**: control over passwords, access, who is overseeing IT?
- **HR procedures** – don’t hire people with questionable backgrounds
- **Analytical review and budget monitoring**: look for anomalies
**Bribes/Kickbacks and Conflicts**

**PREVENTION**
- Policies to prohibit gifts, loans or discounts from vendors
- Purchasing policies and procedures to avoid “restricted “competition
- Review vendor “ownership” – any conflict?
- Annual disclosure statement of potential conflicts

**DETECTION**
- Same vendor used too often (tips and complaints)
- Costs more than market
- No bid contract
- Compare vendor addresses to employee addresses
- Extravagant lifestyle or drug/alcohol/gambling habits
Cash Fraud: Cash Skimming (off-the books) and Larceny (on-the books)

**PREVENTION**
* Itemized cash receipts
* Segregation of billing and cash receipting duties
* Use of lockbox
* Bonding employees
* Physical securities
* Surprise cash count
* Mandatory vacations and job rotation

**DETECTION**
* Analytical procedures
* Journal entry review
* Independent reconciliations
* Cash account analysis
Accounts Payable Fraud: Check Tampering, Fictitious Vendor

**PREVENTION**

* Independent review of: payment support, distribution of checks, vendor listing and reconciliation of bank account
* Segregate purchasing and AP functions
* Competitive bid
* Use of special check stock paper, typeface or ink to alert bank of check tampering

**DETECTION**

- Bank reconciliation
- Check tampering red flags
- Journal entry review
- Analytical review
- Review of vendor listing
- Positive pay banking (bank verifies checks presented against list of payees and amounts from customer and investigates “off list” checks)
Payroll Fraud: Fictitious Payroll and Expense Reimbursement Schemes

**PREVENTION**
* Segregation of HR and payroll
* Proper personnel file documentation
* Approval of overtime, hours and pay rate changes
* Approval of expense reimbursements and review of backup
* Clear and enforced policies on expense reimbursements

**DETECTION**
* Search for duplicate Social Security number
* Overtime analysis
* Budget monitoring
* Analytical review
* Surprise distribution of payroll at work location
2012 REPORT TO THE NATIONS

Impact of Hotlines

Detection Method
- Tip
- Internal Audit
- Management Review
- Account Reconciliation
- Document Examination
- By Accident
- Surveillance/Monitoring
- Notified by Police
- Confession
- IT Controls
- External Audit
- Other

Percent of Cases

Percentages for Organizations With Hotlines:
- Tip: 60.9%
- Internal Audit: 16.3%
- Management Review: 13.8%
- Account Reconciliation: 4.5%
- Document Examination: 3.0%
- By Accident: 2.8%
- Surveillance/Monitoring: 2.4%
- Notified by Police: 1.7%
- Confession: 1.3%
- IT Controls: 1.3%
- External Audit: 1.0%
- Other: 1.0%

Percentages for Organizations Without Hotlines:
- Tip: 34.6%
- Internal Audit: 12.8%
- Management Review: 16.6%
- Account Reconciliation: 4.8%
- Document Examination: 6.8%
- By Accident: 11.3%
- Surveillance/Monitoring: 1.6%
- Notified by Police: 3.7%
- Confession: 1.8%
- IT Controls: 0.6%
- External Audit: 6.7%
- Other: 1.0%
2012 REPORT TO THE NATIONS

![Source of Tips Chart]

- Employee: 50.9%
- Customer: 22.1%
- Anonymous: 12.4%
- Other: 11.6%
- Vendor: 9.0%
- Shareholder/Owner: 2.3%
- Competitor: 1.5%
Questions?

THANK YOU!