Fraud Prevention and Detection
Dan Acquilano, Associate Examiner
William D. Naylor, CIA, CFE, Senior Examiner
Division of Local Government and School Accountability

Meet the Presenters
Dan Acquilano
William Naylor

What is Fraud?
An illegal act involving obtaining something of value through willful misrepresentation.
Examples of Fraud

• Theft of cash
• Forgery
• Falsifying accounting records
• Theft of service

What is Abuse?

Behavior that is improper when compared with behavior that a prudent person would consider a reasonable and necessary business practice given the facts and circumstances.

Examples of Abuse

• Incurring excessive expenses
• Misuse of municipal equipment or supplies
Implications

• Impose large costs on organizations
• Public confidence and reputation of municipality and/or individuals involved

The Fraud Triangle

Incentive/ Pressure

Management or other employees may have an incentive or be under pressure, which provides motivation to commit fraud.
Incentive/Pressure - Risk Factors

- Personal financial obligations
- Requirements or expectations of third parties
- Personal net worth threatened by financial performance

Rationalization/Attitude

The attitude, character or set of ethical values that allows them to intentionally commit a dishonest act.

Rationalization/Attitude - Risk Factors

- Disregard for internal controls, the need for monitoring or reducing risks
- Behavior indicating dissatisfaction
- Changes in lifestyle
Opportunity

Circumstances exist that provide an opportunity for fraud:

• The absence of controls
• Ineffective controls
• Management override

Opportunity - Risk Factors

Lack of or deficiencies relating to:

• Policies
• Records
• Duties
• Reconciliations
• Oversight

Internal Control

A process effected by the governing board, management and other personnel designed to provide reasonable assurance that:

• Financial reporting is reliable
• Operations are effective and efficient
• Laws and regulations are complied with
Limitations of Internal Control

No matter how well designed, controls can only provide reasonable assurance:

• Errors
• Collusion
• Management override

Cost/Benefit of Controls

The cost of an entity’s internal controls should not exceed the benefits that are expected to be derived.

Prevention vs. Detection

Preventive controls are designed to keep fraud and abuse from occurring in the first place.

Detective controls are designed to detect fraud and abuse that may have occurred.
Steps to Prevention and Detection

• Step #1 – Communication
  Establish, communicate and reinforce expectations for behavior

• Step #2 – Checks and Balances
  Implement and monitor controls

• Step #3 – Follow Through
  Ensure there are consequences

Step #1: Communicate Expectations

Policies
• Code of ethics
• Policies and procedures manuals
• Job descriptions

Lead by Example

Code of Ethics

Establishes standards of conduct to avoid:
• Appearance of impropriety
• Use of position for personal gain
• Private employment in conflict with official duties

Also addresses:
• Confidential information
• Gifts
• Enforcement
Policies
Establish:
• Employee responsibilities
• Limits to authority
• Performance standards
• Control procedures
• Reporting relationships
  Example: Internet and email computer use policy

Leading by Example
Modeling the ethical behavior set forth in the policies.

Effects of a Poor Tone at the Top
A nonexistent or ineffective means of establishing, communicating and supporting the local government’s accountability for public resources and ethics, especially regarding codes of conduct, conflicts of interest and acceptable business practices increases the risk of fraud and abuse.
Step #2: Checks and Balances

Where is the greatest risk?

- External and internal sources
- Opportunity fraud risk factors
- System monitoring issues

Tempting Assets

- Cash
- Fixed assets that are small in size, marketable or lacking in observable identification of ownership

Controls - Cash and Other Desirable Assets

- Limit physical access
  - Cash
  - Check stock and signature plates
  - Information technology system
- Place ID on high-risk inventory
Controls - Segregation of Duties

Separate the basic functions:
  • Authorizing transactions
  • Maintaining records
  • Having custody of assets

Helps prevent errors, fraud and/or abuse from occurring and remaining undetected.

Controls - Monitoring

• Remain alert to the possibility
• Use the IT tools you already have
• Encourage reporting
• Audits

Step #3: Follow Through

• Investigate allegations of fraud or abuse
• Ensure there are consequences
• Maintain transparency
No Consequences
A substantial internal control deficiency that increases the perception of opportunity –

No negative ramifications for fraud or abuse

Unique Fraud Risk Factors
• Management override of controls
• Information technology

Management Override
Management has the unique ability to commit fraud because it is in a position to directly or indirectly manipulate and/or influence records, processes and people.
Information Technology

• Fraud often involves the use of technology
• A thorough understanding and review of IT controls is essential whether IT function is in-house or out-sourced

Common IT Deficiencies

Lack of access controls
• Access rights too broad
• Sign-in passwords not required
• Rights changed without approval
• System cannot be monitored

Monitoring
• Audit logs
• Exception reports

Summary

• Costly, intentional acts
• Pressure, opportunity and rationalization
• Prevention and detection
  • Communication by words and actions
  • Checks and balances that are monitored
  • Follow through
Resources

• Division of Local Government & School Accountability
  www.osc.state.ny.us/localgov/contact.htm
  1-866-321-8503 or (518) 408-4934
  localgov@osc.state.ny.us

• Division of Investigations
  www.osc.state.ny.us/investigations/index.htm
  1-888-672-4555
  investigations@osc.state.ny.us

• Local Official Training Unit
  LocalTraining@osc.state.ny.us

Thank You

Division of Local Government and School Accountability
localtraining@osc.state.ny.us