Fraud Awareness and Prevention

Comptroller of the Commonwealth
Goal of Fraud Awareness and Prevention Training

- Fraud Awareness and Prevention Training is part of The Office of the Comptroller’s mission to assist departments in assuring taxpayers that funds are expended as intended

  - Goal of this session is to raise awareness of fraud risks and methods for prevention and detection

“Think like a taxpayer, because you are one”
Agenda

- Fraud Awareness
- Types of Fraud
- Consequences of Fraud
- Activity
- Fraud Red Flags
- Risks, Red Flags, and Control Examples
- Prevention
- Detection
- What’s Next?
“There is no kind of dishonesty into which otherwise good people more easily and more frequently fall than that of defrauding the government.”

-Ben Franklin
What is Fraud?

- Any intentional illegal acts characterized by deceit, concealment, or violation of trust

- Frauds are committed by individuals and organizations to:
  - obtain money, property, or services
  - avoid payment or loss of services
  - secure personal or business advantage

Source: The Institute of Internal Auditors International Standards for the Professional Practice of Internal Auditing. [www.theiia.org](http://www.theiia.org)
Section 66. Any officer or employee who knowingly violates, authorizes or directs another officer or employee to violate any provision of this chapter, or any rule or regulation promulgated thereunder, or any other provision of law relating to the incurring of liability or expenditure of public funds, shall be punished by a fine of not more than one thousand dollars or by imprisonment in a jail or house of correction for not more than one year, or both.
Embezzlement cases on the rise

http://www.eagletribune.com/

- Often, they are people their employers trust
- They are the last people you would think to be wary of
- Sometimes it's taxpayer money
- It's happened everywhere: at town hall, in a hospital accounting department, at high-tech firms, and even at a church
- "It's usually driven by debt or vices, like gambling," Lawrence police Chief John Romero said. "We've had a few cases recently."

November 22, 2009
The Fraud Triangle

Opportunity:
- Internal Controls
  - None in place
  - Un-enforced
  - Un-monitored
  - Ineffective
- Too much trust
- Poor “Tone at the Top”
- No segregation of duties

Rationalization:
- “I don’t get paid what I am worth!”
- “Everyone else is doing it”
- “If they don’t know I’m doing it, they deserve to lose the money”
- “I intended to pay it back”
- “Nobody will miss the money”

External Pressure / Motivation:
- Debt, Greed
- Lifestyle Needs
- Illicit Activities: Vices, Gambling, Drugs
- Life Pressures

Internal Pressure / Motivation:
- Pressure to Perform
- Too Much Work
The Fraud Triangle

We have limited control over:
- Pressure
- Rationalization

We have the most control over:
- Opportunity
Who commits fraud?

- People outside the organization
- People in positions of responsibility with the ability to override controls
- Often trusted and respected employees
- People with an understanding of the system and processes
  - “Inside Jobs” are easier
Money? + People? = Fraud
10-80-10 Rule

The 10-80-10 “rule” refers to a general assumption of the breakdown of the population and the likelihood of fraud occurrences:

- **10%** of the population will NEVER commit fraud. This is the type of person that will go out of their way to return items to the correct party.

- **80%** of the population might commit fraud given the right combination of **opportunity**, **pressure**, and **rationalization**.

- **10%** of the population are actively looking at systems and trying to find a way to commit fraud.

*Source* NASACT and the Oregon State Controller’s Division
Average life of a fraud

- Average duration of 18 months†

- 91 percent of perpetrators did not stop at one single fraudulent transaction*

*Source: Association of Certified Fraud Examiners 2010 Report to the Nation on Occupational Fraud & Abuse. www.acfe.com

*Source: Profile of a Fraudster Survey 2007, KPMG
What are the concerns for management?

- 32% of executives expect some form of fraud or misconduct to rise in their organizations over the next year

- 65% reported that fraud and misconduct is a significant risk for their industry

- The greatest concern for 71% is the potential for a loss of public trust

KPMG Fraud Survey 2009
What are the concerns for management? (Continued)

- 66% reported that inadequate internal controls at their organizations enable fraud and misconduct to go unchecked
- 33% lacked protocols on how to remedy control breakdowns
- Executives acknowledge room for improvement across most elements of their antifraud efforts:
  - Employee communication and training
  - Technology-driven continuous auditing and monitoring techniques
  - Fraud and misconduct risk assessment

KPMG Fraud Survey 2009
“It can’t happen in my office”
<table>
<thead>
<tr>
<th>News Title</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Texas Couple Indicted On Charges Of Embezzling More Than $220K From Non-Profit Health Care</td>
<td></td>
</tr>
<tr>
<td>Massachusetts City Employee Accused Of Embezzling More Than $1/2 Million</td>
<td></td>
</tr>
<tr>
<td>Former South Carolina DMV Worker Charged In $300K Embezzlement Scheme</td>
<td></td>
</tr>
<tr>
<td>Former Ohio Municipal Deputy Treasurer Sentenced For $3 Million Embezzlement</td>
<td></td>
</tr>
<tr>
<td>Pennsylvania Municipal Manager Charged With Embezzling $178K</td>
<td></td>
</tr>
<tr>
<td>Former Longtime City Employee In Washington State To Plead Guilty Of Embezzling $1.3 Million</td>
<td></td>
</tr>
<tr>
<td>Pennsylvania Municipal Utility Worker Sentenced In $475K Embezzlement Case</td>
<td></td>
</tr>
<tr>
<td>Former Louisiana Non-Profit Bookkeeper Pleads Guilty To Embezzling $1 Million</td>
<td></td>
</tr>
<tr>
<td>Former Louisiana Non-Profit Bookkeeper Pleads Guilty To Embezzling $1 Million</td>
<td></td>
</tr>
<tr>
<td>Former Louisiana Non-Profit Bookkeeper Pleads Guilty To Embezzling $1 Million</td>
<td></td>
</tr>
<tr>
<td>Former Louisiana Non-Profit Bookkeeper Pleads Guilty To Embezzling $1 Million</td>
<td></td>
</tr>
<tr>
<td>Former Louisiana Non-Profit Bookkeeper Pleads Guilty To Embezzling $1 Million</td>
<td></td>
</tr>
<tr>
<td>North Carolina Couple Charged With Embezzling $360K From Church</td>
<td></td>
</tr>
<tr>
<td>Former Illinois Youth Football League Treasurer Charged With Embezzling $112K</td>
<td></td>
</tr>
<tr>
<td>Former Mississippi Municipal Worker Indicted For $900K Embezzlement Scheme</td>
<td></td>
</tr>
<tr>
<td>Former Indiana Crime Stoppers Treasurer Charged With Embezzling $100+K</td>
<td></td>
</tr>
<tr>
<td>Montana Woman Pleads Guilty To Embezzling &quot;Hundreds of Thousands&quot; From School</td>
<td></td>
</tr>
<tr>
<td>Former North Carolina Sheriff Lieutenant Accused Of Embezzling Nearly $100K</td>
<td></td>
</tr>
<tr>
<td>Illinois Non-Profit Exec Pleads Guilty To Embezzling $667K</td>
<td></td>
</tr>
</tbody>
</table>
“It can’t happen here”

JULY 12, 2010

- A DOC lieutenant indicted on charges of financial conflict of interest, two counts of procurement fraud, and three counts of larceny

- These charges are in addition to those brought against the lieutenant in 2008 for stealing more than US $100,000 in state money to buy firearms and other law enforcement equipment for personal use

- The new charges stem from the lieutenant’s relationship with a firearms vendor — selected with the lieutenant’s help — who won a contract to provide the DOC with firearms, ammunition, and accessories

- The lieutenant allegedly bought sporting goods and other items using a personal line of vendor credit without a DOC purchase order with the understanding that the cost would be deducted from the DOC’s line of credit

- Prosecutors also allege that the lieutenant stole and sold ammunition in exchange for credit at major retailers as well as checks made payable to him
A Multi-million dollar, international fraud and money laundering scheme targeted vendors of state governments from West Virginia, Kansas and Ohio, as well as the Commonwealth of Massachusetts, which resulted in the diversion of $3.379 million in state payments routed to fraudulent bank accounts.

The fraudsters were able to hijack legitimate vendor payments using information acquired through the Internet and otherwise to complete direct deposit authorization forms for Deloitte Consulting LLP, Unisys Corporation, and Electronic Data Systems, Inc.:

- Targeted state vendors who routinely received significant payments
- Created phony entities with names similar to the legitimate vendors
- Produced fraudulent bank accounts in the names of the targeted vendors
- Mailed authorization forms and voided starter checks from fraudulent accounts
- The unsuspecting states sent the payments to the fraudulent bank accounts
Types of Fraud
Types of Fraud—
“The Big Three”

- **Asset Misappropriation**
  Theft of cash, inventory, services, and other assets
- **Corruption**
  Conflict of Interest, Bribery
- **Fraudulent Statements and Reporting**
  Financial and Non-financial

**Distribution of Fraud Across the “Big Three”**

- Asset Misappropriation: 88.7%
- Corruption: 27.4%
- Fraudulent Statements: 10.3%

Source: Association of Certified Fraud Examiners 2010 Report to the Nation on Occupational Fraud & Abuse. [www.acfe.com](http://www.acfe.com)
Q. Which of the following categories of fraud and misconduct pose the most significant risk to your organization? (Results by industry)
Uniform Occupational Fraud Classification System

Source: Association of Certified Fraud Examiners 2010 Report to the Nation on Occupational Fraud & Abuse. www.acfe.com
Types of Fraud – Asset Misappropriation

- Asset misappropriations include the misuse or theft of assets
  - Money
  - Inventory
  - Property / Fixed Assets
  - Information (Personally Identifiable Information “PII”)
    - See information regarding Executive Order 504
Types of Fraud – Asset Misappropriation

- **Internal**
  - Cash Theft
  - Accounts Receivable (phony customers or credits)
  - Inventory Fraud (theft)
  - Accounts Payable Frauds (phony suppliers)
  - Payroll Frauds (ghost employees, stealing “time”)
  - Inflated Expense Reports by Employees

- **External**
  - Theft
  - False Claims, Delivery of Goods or Services for ineligible Receiver
  - Vendor Fraud
    - Payroll Frauds
    - Inflated Expense Reports by Employees of Vendor
    - Sub Recipients
    - Mis-charging
Types of Fraud – Corruption

- Abuse of Power
- Management Override
- Collusion
- Blackmail
- Conflict of Interest
- Bribery
- Illegal Gratuity
- Extortion
- Kickback
Types of Fraud – Fraudulent Statements

- Misapplication of accounting rules
  - Mischaracterization as "one-time" expenses

- Misrepresentation or omission of information

- Vendor / Sub-Recipient False Reporting
  - Inflating Costs
Types of Fraud – Social Engineering

- Social engineering is the act of manipulating people into performing actions or divulging confidential information.

- Is too much of your information available to the public?
  - Forms? Job Aids? “Decoder Rings”
    - Instructions on what information is needed, how to complete, and who to send to?

- Employees want to be helpful
  - Develop protocols for dealing with information requests
  - Practice “Professional Skepticism”
From: WEBMAIL UPGRADE SERVICE CENTER [mailto:info@service.ma.us]
Sent: Monday, May 04, 2009 8:04 AM
To: undisclosed-recipients
Subject: Verify And Update Your State.ma.us Email Account.

Verify And Update Your State.ma.us Email Account.

Dear State Email Account User:
We are sending this mail to you in regards of congestion due to our services, due to the congestion of State users, state.ma.us will be shutting down all unused Accounts, You will have to confirm your E-mail by filling out your Login Information below to our webmail upgrade services.

*USERNAME:

*PASSWORD:

*DATE OF BIRTH:

We thank you for your prompt attention to this matter. Please understand that this is a security measure intended to help protect your account. We apologise for any inconvenience.

Warning Code: VX2G99AAJ

Thank you for using state.ma.us
The state.ma.us Team
Scareware
Don’t be a victim of Social Engineering

- Be suspicious of unsolicited phone calls or emails from individuals asking about employees or other internal information.

- If an unknown individual claims to be from a legitimate organization:
  - Try to verify his or her identity directly with the company.
  - Get contact information from previous statements or your vendor contact records.

- Do not reveal personal or financial information in email and do not respond to email solicitations for this information - This includes following links sent in email.

- Pay attention to the URL of a web site.

- Don’t open attachments from unknown individuals.

- Install anti-virus software, firewalls, and email filters.
Don’t be a victim

Trust, But Verify
&
Practice Professional Skepticism
Consequences of Fraud
Consequences of Fraud—Financial Cost

- Losses estimated to be 5 percent of revenue*
- Loss of assets
- Potential loss of future funding
- Potential fines, repayment of funding

*Source: Association of Certified Fraud Examiners 2010 Report to the Nation on Occupational Fraud & Abuse. [www.acfe.com](http://www.acfe.com)
FY 2009 Revenue

FY 2009
Government Fund Types Revenues in Millions

- Taxes, $18,513
- Federal reimbursements, $9,139
- Federal grants, $2,646
- Motor vehicle licenses and registrations, $383
- Assessments, $894
- Lotteries, $4,649
- Fees, investment earnings, etc, $2,800

$ 1.9 Billion
Headlines you won’t see…

MOST STATE EMPLOYEES HAVE A PRODUCTIVE DAY

“Kevin was a few minutes early today and did a fine job” says boss. Ticker Tape Parade Set for Saturday Complete Coverage Pages 3-5
Consequences of Fraud - Damage to Public Image / Reputation

- Traditional News Media
  - Newspapers
  - TV
  - Radio

- Electronic Word of Mouth
  - Twitter
  - Facebook
  - Blogs
  - Message Boards
    - Globe & Herald
Scenario

- You are the town purchasing director assigned the task of selling surplus property on eBay.
  - Could fraud occur?
  - What are the potential consequences?

- Think you are busy now? Put this on your plate…
Official accused of selling town property on eBay
November 2009

- Town purchasing director sold surplus equipment on eBay and had winning bidders write the checks out in his name

- Amount stolen close to $30,000. According to police reports, he said he stole to buy his girlfriend an engagement ring - He also claimed depression

- Actions were first brought to light on Nov. 10, when a resident asked Assistant Town Manager why the purchasing director was asking people to make checks out to him and not the town

- Town Manager apologized for the "cloud" the scandal has cast over the town

Continued…
The town did have procedures in place to track fixed assets, and had begun to improve on those when the embezzlement occurred.

Selectmen last week charged the town's Audit Committee with investigating and making recommendations on how to improve internal controls.

Town Manager: “We will, of course, work diligently to design and implement new procedures that will make a reoccurrence of what happened very, very difficult.”

The town is also looking at various ways to recover the stolen money: currently targeting frozen retirement funds, seeking restitution through the courts, and filing an insurance claim.

Continued…
Purchasing director had worked for town since January of 2008 - He had an unblemished 20-year military record, he worked for several years in state government, and he came with excellent references

"We did a thorough job in checking out his background. There was nothing to indicate in his behavior or work product that he was capable of the illegal activity he engaged in."

Town Manager called the embezzlement "disheartening on both a personal level and to all of our employees who have worked so hard to improve and put in place proper financial policies and procedures."
Consequences of Fraud - Internal Consequences

- Damages Organizational Integrity / Credibility
- Damages Morale
- Creates an Environment of Mistrust
- Increases focus from Everyone
- Nobody wants to be under that “Cloud”
Consequences of Fraud -
Consequences to You if Caught
Activity
Fraud Red Flags
Do you have....?

- Large amounts of cash in hand
- Small items with a high cash value (laptop, thumb drive, Blackberry)
- Easily convertible assets (tools, vehicles, PII)
- Lack of segregation of duties
- Management with ability to override
- Managers and Employees with access to significant assets
- Poor physical safeguards over cash and other assets
- Lack of mandatory time off for employees performing key control functions
- Inadequate supervision, especially where employees are in remote locations
- Too much information on your website
Do you have....?
Lack of segregation of duties

Same person:

- Opens mail with checks
- Records checks received
- Prepares bank deposit
- Deposits money into bank
- Reconciles bank statements
Do you have….?
Resource Constraints

- Not enough staff to perform the current work
- Not enough staff to supervise work performed
- Lack of funds for monitoring tools
- Lack of staff time to devote to anti-fraud activities
Do you have….?
Times of change

- Change in leadership
- Reorganization
- Layoffs
- Upgrades / Promotions
- New programs without new resources
Do you have....?

External Pressure on Employees

Recognize and acknowledge the pressure when possible.

- Financial Issues (Mortgage, Student Loans)
- Medical Bills
- Divorce
- Child Support
Do you have….?
Changes in Employees Behavior

- Unwilling to take vacation / time off
- Working off hours: early, late, weekends
- Refusing promotion to a different area
- Overly protective of information and reluctant to train others
- Social relationship with vendor
- Change in lifestyle, suddenly living beyond means
Risks, Red Flags, and Controls
# Risks, Red Flags and Controls

<table>
<thead>
<tr>
<th>Risk</th>
<th>Red Flags</th>
<th>Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraudulent billing</td>
<td>Fraudulent invoices</td>
<td>Site inspections</td>
</tr>
<tr>
<td></td>
<td>Mischaracterized expenses (personal vs. business)</td>
<td>Confirmation of delivery</td>
</tr>
<tr>
<td></td>
<td>Inflated billing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Double billing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Lack of proof of delivery</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Equipment / people not on jobsite</td>
<td></td>
</tr>
<tr>
<td>Product substitution</td>
<td>Complaints about quality</td>
<td>Adequate project monitoring and oversight</td>
</tr>
<tr>
<td></td>
<td>Poor quality construction</td>
<td>Independent testing</td>
</tr>
<tr>
<td></td>
<td>Lack of inspection</td>
<td>Agency verification of inspection reports</td>
</tr>
<tr>
<td></td>
<td>False inspection report</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Allegations of bribery of inspectors</td>
<td></td>
</tr>
</tbody>
</table>
# Risks, Red Flags and Controls

<table>
<thead>
<tr>
<th>Risk</th>
<th>Red Flags</th>
<th>Controls</th>
</tr>
</thead>
</table>
| Collusive bidding, price fixing or bid rigging | Apparent connections between bidders: common addresses, personnel, or telephone numbers  
Different contractors make identical errors on bids.  
Tailored Specifications (e.g., specific or restrictive requirements in files which seems to restrict eligibility)  
Similar pricing  
Consistently high pricing                                           | Adequate vendor pre-screening  
Independent price verification and pricing analysis |
| Conflict of interest                           | Apparent connections between employees and vendors:  
  - Common addresses or telephone numbers  
  - Tax ID  
  - Ownership interest  
Unnecessary purchases  
Sole source justification                                           |  - Adequate vendor screening  
  - Data analysis / tools  
  - Formal procurement process  
  - Codes of conduct |
### Risks, Red Flags and Controls

<table>
<thead>
<tr>
<th>Risk</th>
<th>Red Flags</th>
<th>Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Falsified wages</td>
<td>Large or unusual overtime payments to selected employees</td>
<td>Review of supporting documents</td>
</tr>
<tr>
<td></td>
<td>Large or unusual hours worked in a given pay cycle</td>
<td>Adequate time tracking mechanisms</td>
</tr>
<tr>
<td></td>
<td>Time card hours differ from job order hours</td>
<td>Authorization and approval of hours worked</td>
</tr>
<tr>
<td></td>
<td>Hours on payroll reports differ from time-card hours or job order</td>
<td>Multiple sources of information</td>
</tr>
<tr>
<td></td>
<td>Number of days worked and amount of salary are inconsistent with occupation</td>
<td></td>
</tr>
<tr>
<td>Social Engineering</td>
<td>Unexpected inquires from unverified callers</td>
<td>Verification identity with organization</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Develop a procedure for dealing with information requests and the type of information you can and cannot give out</td>
</tr>
</tbody>
</table>
Prevention
Most Important Contributing Factor to Fraud

Source: Association of Certified Fraud Examiners 2010 Report to the Nation on Occupational Fraud & Abuse. www.acfe.com
Internal Controls

- Update your Internal Control System (per Chapter 647 of the Acts of 1989), consisting of the Internal Control Plan and the policies and procedures that govern your daily activities

- Attend our “Risk Management” course for Internal Control guidance
Tone at the Top

The atmosphere created at the top affects the attitude of all employees:

- Employees witness what their bosses are doing
- Zero tolerance for unlawful, unethical, or questionable behavior
- Reward employees for integrating personal and organizational loyalty
- Write It (Policies and Procedures, Memos)
- Communicate It (Meetings, Trainings)
- Demonstrate It (Lead by Example)
Ethics Statement / Code of Conduct

- **Define** the culture
- **Set** expectations
- **Remind** employees about their roles and responsibilities for maintaining an ethical work environment
- **Maintain** awareness of reporting mechanisms available to employees
- **Reinforce** the ramifications of improper or unacceptable behavior in order to deter others from similar actions

**State Ethics Mandatory Education and Training Requirements**
Training & Communication

Training:
- Training as standard part of new employee orientation
- Annual certification for existing employees

Communication:
- Why don't employees tell what they know - Because no one asks?
- Interview employees, ask if they suspect fraud in the organization
- Ask employees - “How would you do it?”
Policy and Procedure

- Be certain to have them in writing
- Make sure they are readily accessible
- Train
- Enforce
- Monitor for effectiveness
- Update
- Have everyone sign off that they received and read
Segregation of Duties

Verify that segregation of duties are in place:

- Apply consistently across the agency and in all locations.
- Example - Reconciliation of balances and activities is performed by someone who does not report them.

If resource constraints prevent adequate segregation of duties:

- Cross-train
- Job rotation
- Add additional sign off / review
- Think creatively; share duties with other areas / units / departments
All new users must be adequately trained on relevant fiscal policies and should not be allowed to enter or approve transactions unless they have undergone training.

Sharing of security id’s is prohibited.

Monitor staff use of MMARS regularly.
Hard Copy / Paper Files

Physical Access to paper files:
- Are paper files with PII locked up or out in the open for all to see?
- Contracts
- Pay stubs
- Tax files
- Personal files (credit card bills)

Disposal:
- Do you throw paper with PII the in recycling or trash barrel? – Dumpster Divers
- Do you have a shredding policy?

**MGL CHAPTER 93 I. DISPOSITIONS AND DESTRUCTION OF RECORDS**
Information Technology

- **Logical Access to Systems**
  - Is it appropriate? Are the roles appropriate?
  - Is it reviewed?
  - Is it terminated in a timely manner?
  - Is sensitive data encrypted?
  - Do sessions time out?
  - Do passwords expire? Can they be repeated?

- **Physical Access**
  - How secure is your server room?
  - Do you have a Laptop, equipment inventory system?
  - Does your copy machines store a digital image of every document scanned or copied?
  - Is weekend work allowed or need to be pre-approved?
Employee Screening

- Past Employment Verification
- Criminal Conviction Checks (CORI)
- Reference Checks
- Education and Certificate Verification
- Get the Consent of the Candidate

Executive Branch Application for Employment
Initial Detection of Fraud

Source: Association of Certified Fraud Examiners 2010 Report to the Nation on Occupational Fraud & Abuse. www.acfe.com
Whistleblower Mechanisms

Commonwealth Hotline Numbers:

- **Inspector General**  (800) 322-1323
  Confidential hotline to report suspected fraud, waste or abuse in government

- **Attorney General - Fair Labor Helpline**  (617) 727-3465
  To report violations of minimum wage and overtime laws and requirement for timely payment of wages

- **Division of Unemployment Assistance**  (800) 354-9927
  To report unreported wages or persons collecting benefits while working

- **Office of the State Auditor**  (617) 727-6200
  For state agencies to report variances, shortages or thefts of funds or property
Whistleblower Protections

Chapter 149, Section 185 of the General Laws protects public employees who wish to make disclosures to expose violations of law or risk to public health, safety or environment in a “whistleblower” mode.

- **Who is Protected?**
  - Employees of the Commonwealth

- **What are whistleblowers protected from?**
  - Firing
  - Suspension
  - Demotion
  - Any adverse employment action being taken as a reprisal

- **What kinds of disclosures are protected?**
  - Disclosure of any activity or practice that is in violation of a law, rule or regulation, or poses a risk to public health, safety or the environment
Deterrence

A fraudster’s willingness to commit fraud is inversely proportional to their perceived risk of being discovered.

Those who perceive they will be caught engaging in fraud are less likely to commit it.
Reconciliation
Let them know someone is watching and checking!

- Bank statements
  - Review all documentation and reconciliations for unusual entries or deviations from programmatic purposes
  - Check for corrections and amounts that appear too high or low
  - Flag and review all management overrides
  - Spot check for round numbers or multiple payments in same cycle for same amount/same recipient (absent a lease or recurring payment)

- DocDirect Reports
  - Payroll Reports
  - Receivables

- Monthly Equipment / Supply Inventory
Data Analysis

- Don’t be a “D.R.I.P.” = Data Rich, Information Poor
- Detect anomalies, trends, risk indicators
  For example, Multiple payments to the same vendor in a month.
- Continuous auditing (monitoring)
- Exception reports
- User activity reports
  - Look for activity from an unexpected user
  - Is the same employee creating and submitting:
    The same document?
    Encumbrances and payment documents?
Program Designed to Minimize Fraud, Waste, and Abuse

Figure 1: Program Designed to Minimize Fraud, Waste, and Abuse

Source: GAO.
What’s Next?
Provide taxpayers assurance that tax dollars are spent for their intended purposes:

- In times like these we are defending our program missions and budgets
- The public demands greater transparency
- Agencies and their personnel that ignore fraud face negative publicity
Provide taxpayers assurance that tax dollars are spent for their intended purposes:

- Tighten internal controls
- Document all policies and procedures
- Segregate duties
- Implement an anti-fraud strategy
- Set the right tone – your behavior influences others
- Adhere to policies and procedures
- Report violations
**Fraud Risk Assessment Template**

**Chart it out:** *Managing the Business Risk of Fraud: A Practical Guide*

- Fraud Risk
- Scheme / Scenario
- Potential People Involved
- Likelihood
- Significance
- Inherent Risk
- Control Activity
- Control Type

**Example A:**

<table>
<thead>
<tr>
<th>Identified Fraud Risks and Schemes (1)</th>
<th>Likelihood (2)</th>
<th>Significance (3)</th>
<th>People and/or Department (4)</th>
<th>Existing Anti-fraud Controls (5)</th>
<th>Controls Effectiveness Assessment (6)</th>
<th>Residual Risks (7)</th>
<th>Fraud Risk Response (8)</th>
</tr>
</thead>
</table>

**Example B:**

<table>
<thead>
<tr>
<th>Owner</th>
<th>Fraud Risks</th>
<th>Controls</th>
<th>Monitoring</th>
<th>Likelihood</th>
<th>Impact</th>
</tr>
</thead>
</table>
| Construction Department | Design & build defects (inferior material used & construction not performed per specifications).  
• Reputation risk (injury or fatality at site).  | • Execute construction contract with detailed scope of work (specifications).  
• Periodic site visitations by architects, local building inspectors, engineers, commission agents, and owner’s construction representatives are made to ensure job is on schedule and built per specifications and code.  | • Construction Department  
• Legal  
• Internal Auditing  | M                       | H                  |
Available CTR Resources

Please visit the Fraud Prevention section of our Internal Controls Page for:

**Tri-fold Brochure available for distribution to staff**

**Toolkit for Departments (to Combat Fraud, Waste and Abuse)**

- Issued November 2009
- Covers common “Red Flag” or likely Fraud Indicators experienced by government entities
- Contains a Checklist for Departments to Combat Fraud, Waste and Abuse

[Home > Business Functions > Quality Assurance > Internal Controls](#)
### Checklist for Departments to Combat Fraud, Waste and Abuse

<table>
<thead>
<tr>
<th>Who Should Perform</th>
<th>Item Checked</th>
<th>Tools/Resources</th>
</tr>
</thead>
</table>
| Management         | Each state agency should have a Code of Conduct that meets or exceeds the provisions of MGL Chapter 268A, promotes the highest standards of ethical behavior and is distributed to all employees. | **MGL Chapter 268A**  
Examples  
NAGE Code of Conduct:  
nage.pdf (133 KB)  
Manager’s Code of Conduct link:  
**Manager’s Code of Conduct**  
Ethics.org’s Resource Center:  
**Ethics Toolkit** |
### Checklist for Departments to Combat Fraud, Waste and Abuse

<table>
<thead>
<tr>
<th>Who Should Perform</th>
<th>Item Checked</th>
<th>Tools/Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td><strong>Conduct a Fraud Risk Assessment</strong> to identify where fraud may occur. A fraud risk assessment should consider relevant fraud schemes and scenarios and map them to mitigating controls. <strong>Fraud risks should be included in the enterprise risk assessment conducted as part of your Internal Control Plan</strong> development. COSO's Enterprise Risk Management–Integrated Framework describes the essential ERM components, principles, and concepts for all organizations, regardless of size. The Inspector General has issued an updated guide on developing fraud prevention policies and programs.</td>
<td>Appendix D - Institute of Internal Auditor’s <strong>Managing the Business Risk of Fraud</strong> has a risk assessment framework. <strong>COSO's Enterprise Risk Management Framework</strong> is used in the Comptroller’s Risk Management training offering. Sign up for this training at the Comptroller’s web site: <strong>Training and Meeting Schedule</strong>. <strong>IGO Guide on Fraud Prevention</strong></td>
</tr>
</tbody>
</table>
# Checklist for Departments to Combat Fraud, Waste and Abuse

<table>
<thead>
<tr>
<th>Who Should Perform</th>
<th>Item Checked</th>
<th>Tools/Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Financial</strong></td>
<td>Establish process to verify that all changes to vendor records (name, address change, bank account) are submitted by an authorized vendor signatory, and approved by an agency signatory. This is to prevent theft or misappropriation of funds.</td>
<td>See Comptroller policy: <a href="#">Vendor/Customer File and W-9s</a>.</td>
</tr>
<tr>
<td><strong>Procurement</strong></td>
<td>Ensure goods and services are bought only when needed. This should be reviewed by someone who does not perform the inventory or purchase the goods.</td>
<td>Take regular inventories of goods. An example of an asset inventory spreadsheet for information technology is published by the University of Colorado for its departments. This can be customized for any good or commodity.</td>
</tr>
<tr>
<td><strong>Procurement</strong></td>
<td>Ensure goods purchased are received by someone who does not order them.</td>
<td><a href="#">The Federal Aviation Administration (US DOT)</a> has a good example of receiving reports with signoffs that can easily be replicated.</td>
</tr>
</tbody>
</table>
# Checklist for Departments to Combat Fraud, Waste and Abuse

<table>
<thead>
<tr>
<th>Who Should Perform</th>
<th>Item Checked</th>
<th>Tools/Resources</th>
</tr>
</thead>
</table>
| Procurement        | Establish process to check all bidders/vendors/contractors for debarment or exclusion from federal awards, suspended licenses, etc., as directed by the Operational Services Division’s Procurement Information Center. Also require vendors/contractors to submit copy of valid license with bids | OSD’s [Procurement Information Center](#)  
Federal Sites:  
[Excluded Parties List System](#) – Contains parties that are excluded from receiving Federal contracts,  
[List of Excluded Individuals/Entities](#) - Listed parties are excluded from participation in the Medicare, Medicaid and all Federal health care programs.  
State Sites:  
[DCAM Debarred Contractor’s List](#) - This list consists only of individuals and firms debarred by the Division of Capital Asset Management.  
The Office of the Attorney General maintains a separate list of additional individuals and firms debarred by that office that is available in the Central Register or by contacting the AGO directly at (617) 727-2200 x. 3277.  
[DIA Stop Work Orders](#) – Listed businesses are prevented from bidding or participating in any state or municipal funded contracts for a period of three (3) years.  
[DPL License Check](#) - Check contractors here for valid professional licenses and/or disciplinary actions.  
[DCAM Certified Prime Contractors/Sub-bidders](#) This lists firms that are allowed to bid on state construction projects.  
[Mass Med Board](#) - Check the Massachusetts Board of Registration in Medicine site for [Online Physician Verifications](#). |
Questions?

Comptroller Help Desk

617-973-2468

Comptroller.info@state.ma.us