State of Vermont
Department of Finance and Management

Business Process:	**Fraud Awareness**	**Issue Date: Number:**	**June 2017 BP-11**
Topic:	**Internal Control - Best Practices**	**Revision Date:**	**N/A**
Applicable To:	**All State Agencies, Departments, And Offices**	**Page:**	**1 of 6**

Objective

To provide guidance and recommendations to support departments in their efforts to establish and maintain controls and procedures to aid in the prevention and detection of fraud, waste and abuse.

Definitions of Fraud, Waste and Abuse

For purposes of this document, the terms **fraud** or **fraudulent** include fraud, waste and abuse as defined below.

Fraud: Deliberate act and the intentional misrepresentation, concealment, or omission of the truth for deception or manipulation to the detriment of a person or an organization. ***Occupational fraud*** is the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets. Legally, fraud can lead to a variety of criminal charges including theft, embezzlement and larceny.

Waste: Significant loss or misuse of resources; careless or thoughtless expenditure, consumption, mismanagement or squandering of resources to the potential detriment of the State; incurring unnecessary costs because of grossly deficient or negligent practices, controls or decisions. *Waste does not necessarily lead to an allegation of fraud or other violations of law.*

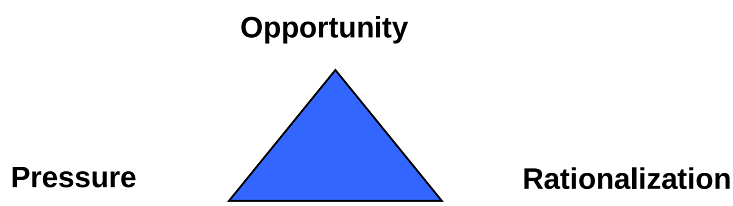
Abuse: Grossly excessive or improper use of something in a manner contrary to the natural or legal rules for its use; intentional destruction, diversion, manipulation, misapplication or misuse of State resources; improper or wrongful use of one's position or authority. *Abuse does not necessarily lead to an allegation of fraud or other violations of law.*

Examples of fraud, waste and abuse include, but are not limited to:

- Forgery or alteration of documents (e.g., checks, contracts, purchase orders, invoices, timesheets, expense accounts, etc.);
- Misrepresentation of information on documents (e.g., financial records, timesheets, expense accounts, employment history, etc.);
- Misappropriation, theft, unauthorized removal or willful destruction of funds, securities, property, equipment, supplies, or any other asset;
- Impropriety in the handling or reporting of financial transactions;
- Authorizing or receiving payment for goods not received, services not performed, hours not worked or expenses not incurred;
- Misuse of authority or knowledge of State operations for personal gain or benefit of others;
- Unauthorized disclosure or sale of confidential information to external parties, or use of this information in the conduct of an outside business activity;
- Engaging in an outside business activity that is inconsistent, incompatible or in conflict with official duties (re: *conflict of interest*);
- Any computer-related activity involving the alteration, destruction, forgery or manipulation of data for fraudulent purposes;
- Accepting or seeking anything of value from contractors, vendors, or persons providing goods and/or services to the State.

Why Fraud Occurs

The **Fraud Triangle** is a classic model used to describe and explain the nature of fraud. In nearly all fraud cases, these three elements are present to some extent; understanding the triangle can enhance an organization's fraud prevention efforts.



1. **Pressure:** A non-shareable pressure or perceived pressure, typically economic, which motivates an individual to consider an illegal act as a solution to their problem. The incentive for an individual to commit fraud can range from unrealistic deadlines or performance expectations, to economic hard times, to personal vices such as alcohol, drugs or gambling.
2. **Opportunity:** Circumstances within an organization that enable an individual to perpetrate a fraud, generally through weaknesses in internal controls (e.g., inadequate separation of duties, ineffective supervision or review, absence of approvals, management's ability to override controls, etc.).
   - Minimizing an individual's **opportunity** to commit and conceal fraud is the only element over which organizations have significant control.
3. **Rationalization:** A frame of mind that allows the individual to rationalize and justify their dishonest actions (e.g., "*No one will ever know*", "*These rules don't apply to me*", "*I'll pay it back later*", "*I'm underpaid and deserve this*", "*Everybody's doing it*", "*It's a perk of the job*", etc.).

Characteristics of Fraud

- The median duration of occupational fraud schemes was 18 months before detection.
- Occupational fraud is far more likely to be detected by tip than any other means; other detection methods include management review, internal audit, external audit, by accident and account reconciliation.
- Lack of internal controls and override of existing internal controls were cited as the primary factors that allowed fraud to occur.
- Most fraudsters have never been previously charged or convicted of a fraud-related offense.
- The most common behavioral red flags displayed by fraud perpetrators were: living beyond their means, experiencing financial difficulties, control issues (unwillingness to share duties) and unusually close association with vendor/customer.
  - Red flags are possible warning signals but do not indicate guilt or innocence.

How Fraud is Committed

Awareness of how fraud may be committed is an important factor in understanding an organization's exposures to fraud; common fraud schemes in government agencies include:

Category/ Scheme	Description	Examples
Corruption	Any scheme in which an employee uses their influence in business transactions in a way that violates their duty to their employer in order to obtain a benefit for themselves or someone else.	▪Paying or receiving bribes (e.g., invoice kickbacks, bid rigging) ▪Engaging in conflicts of interest (e.g., purchasing/sales schemes) ▪Extorting illegal payments or accepting illegal gratuities.
Billing	Any scheme in which a person causes his or her employer to issue a payment by submitting invoices for fictitious goods or services, inflated invoices, or invoices for personal purchases.	▪Employee creates a shell company and bills employer for nonexistent services. ▪Employee purchases personal items, submits invoice to employer for payment.
Non-Cash	Any scheme in which an employee steals or misuses non-cash assets of the organization.	▪Employee steals inventory from a warehouse or storeroom. ▪Employee steals or misuses confidential customer financial information.
Skimming	Any scheme in which cash is stolen from an organization *before* it is recorded on the organization's books and records.	▪Employee accepts payment from a customer but does not record the sale.
Cash-on-Hand	Any scheme in which the perpetrator misappropriates cash kept on hand at the organization's premises.	▪Employee steals cash from a safe.
Expense Reimbursements	Any scheme in which an employee makes a claim for reimbursement of fictitious or inflated business expenses.	▪Employee files fraudulent expense report, claiming personal travel, nonexistent meals, etc.
Check Tampering	Any scheme in which a person steals his or her employer's funds by forging or altering a check on one of the organization's bank accounts, or steals a check the organization has legitimately issued to another payee.	▪Employee steals blank checks, makes them out to himself or an accomplice. ▪Employee steals outgoing check to a vendor, deposits it into his or her own bank account.

Category/ Scheme	Description	Examples
Payroll	Any scheme in which an employee causes his or her employer to issue a payment by making false claims for compensation.	▪Employee claims overtime for hours not worked. ▪Employee adds ghost employees to the payroll.

Best Practices: Fraud Prevention & Detection

❖ Control Environment ("Tone at the Top")

- Establish a clear message that fraud, waste and abuse will not be tolerated, nor will any attempt to conceal fraudulent activity.
- Managers acknowledge that fraud *can* occur and that it is most often committed by those in positions of trust; denial and willful blindness are often contributing factors in significant fraud cases. **"Trust is an emotion, not a control."**
- Inform all employees of the expectation for them to report suspected fraud, waste or abuse; encourage employees to be vigilant in their efforts.
- Tell employees to whom (i.e., supervisor, manager, department head, etc.) they should report suspected wrongdoing and how this information can be communicated.
- Establish protocols for those who have been designated to receive reports of fraud.
- Let employees know that any individual (i.e., employee, vendor, customer, contractor, etc.) suspected of wrongdoing will be treated equally without regard to the person's title, position, length of service, relationship to the State, or any other perceived mitigating circumstance.
- Be clear that any type of retaliation against employees or others who report suspected fraud, or provide information concerning suspected fraud, will not be tolerated (refer to Whistleblower Protection statute). Likewise, reports of fraud made in bad faith (i.e., *reporting of information known to be false but representing it as factual and accurate*) will not be tolerated and can result in discipline.

❖ Perception of Detection

- Let employees know that someone is watching them…those who perceive they will be caught engaging in fraud are less likely to commit it.
- Foster a work environment in which employees and others expect that dishonest acts will be detected by management, monitoring techniques, other employees, or the auditors.

❖ Assess the Risk

While all employees have an expectation to report suspected fraud, managers have the primary responsibility for preventing and detecting fraud and other wrongdoing. For their areas of responsibility, all managers should perform a fraud risk assessment:

- Identify the major exposures to fraud for each area of operation. If there were no internal controls in place, how and by whom could fraud be committed?
- Identify the specific controls currently in place to mitigate the fraud risks identified above. Do these controls adequately reduce the risk of fraud to an acceptable level? If not, implement additional control measures to minimize the risk to a tolerable level.
- If fraud was occurring (*or did occur*) …how would it be detected? What are the indicators that would suggest to a manager that something was not right?

❖ Reduce the Opportunity

Anti-fraud controls help reduce the exposure, cost and duration of occupational fraud:

- **Screen out those likely to commit fraud:** Perform thorough reference and background checks appropriate to the position being filled.
- **Embrace the principle of "Least Privileges":** Limit employees' access to cash, systems, confidential data, equipment, property and other assets to only those with a legitimate business need, necessary to perform their essential job duties.
- **Rotate job duties:** Particularly for those in sensitive or high-risk positions.
- **Anonymous tip line:** Provide employees the opportunity to report suspected wrongdoing anonymously within your department or to the State Auditor's Office Confidential Hotline at 1-877-290-1400 or through their website.
- **Surprise audits:** Surprise audits are an effective, yet under-utilized, tool in the fight against fraud. Surprise audits need not be "formal audits" restricted to the auditors but can be conducted by managers or others independent of the area being reviewed and include activities such as unannounced cash counts, random inspection of assets or inventory items, monitoring transactions for inappropriate activity, verifying secure areas and confidential data are adequately protected, etc.
- **Management review of internal control system:** Periodically test controls to ensure they're operating as designed and providing the intended results.
- **Internal audit units:** Provide independent evaluation of the organization's internal control system and can be an objective source of advice and support to managers and employees.
- **Training/Education:** Sponsor fraud awareness and ethics trainings.

- **Employee support programs:** The Department of Human Resources' Employee Assistance Program (EAP) provides confidential assistance to employees and their family members with personal issues such as financial concerns or problems with alcohol and drugs; use of an EAP can help alleviate the "pressure" (re: *fraud triangle*) to commit fraud.

Related Policies, Laws, and Guidance

Including but not limited to:

- Department of Human Resources:
  Personnel Policy and Procedure Manual:
  - Policy 5.6: Employee Conduct
  - Policy 8.0: Disciplinary Action and Corrective Action
  - Policy 17.0: Employment Related Investigations

  Reporting Fraud: Employee Whistleblower Protection
- Vermont Statutes Annotated:
  - Title 3 V.S.A. § 971 - 978: Whistleblower Protection
  - Title 1 V.S.A. § 317 (42): Definitions; public agency; public records and documents

Notices

- These best practices are intended to support the internal control framework as presented in the Internal Control Standards: A Guide for Managers.
- In consideration of these best practices, the objective should be on adherence and not on rationalizing ways and means for circumvention.
- Nothing in this document shall limit or supersede any applicable Federal or State laws, statutes, bulletins, or regulations.

Sources and References:

- Report to the Nations on Occupational Fraud and Abuse, Association of Certified Fraud Examiners
- Other People's Money: A Study in the Social Psychology of Embezzlement, © 1953 Donald R Cressey
- Let Them Know Someone's Watching - The Journal of Accountancy, © 2002 Joseph T. Wells
- Fraud Awareness for Managers, © 2008 Courtenay Thompson & Associates