Trust, but verify:

A guide for elected officials & appointed boards to prevent fraud

Look inside for our special pullout with three simple techniques to detect fraud

Office of the Washington State Auditor

November 2022

Preventing fraud begins at the top

Fraud occurs when an employee is deliberately deceptive in order to attain personal or financial gain, and it costs businesses billions of dollars every year. While corporate fraud may dominate the headlines, in reality, smaller organizations—including local governments—are more vulnerable to fraud, and their average financial loss is twice that of larger organizations.

Employee fraud often comes as a shock to those charged with oversight of a government when it happens in their own agencies. It shouldn't. Just because fraud hasn't been discovered or possibly hasn't happened, does not mean that your agency is not vulnerable.

Not only can fraud damage your government's finances, assets and hard-earned reputation, it can also affect your government's ability to obtain funding, attract top staff and maintain public trust.

As an elected official or a member of an appointed board, you have a duty to understand your government's operations. You also have a key role to play when it comes to fighting fraud. Boards and other officials have the responsibility to lead by example, which demonstrates to employees that you are committed to preventing, detecting and responding to fraud.

The State Auditor's Office (SAO) created this resource to help you understand your role as an elected official or board member in fighting employee fraud. Throughout this resource, you will find tips for implementing policies and best practices that can help you prevent, detect and respond to fraud in your government.

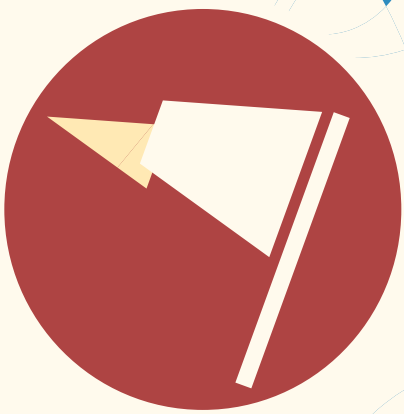
Types of employee fraud

Employee fraud comes in many forms and appears at all levels within your government. An employee intending to commit fraud will often take their time to learn a process fully before they misuse it for personal gain. Examples of fraud schemes used by employees include:

- Pocketing cash or equivalent (inventory/equipment/supplies)
- Not properly recording vacation and sick leave used, and then cashing out leave
- Falsifying reporting of overtime or extra pay, or creating and adding fictitious employees to the payroll
- Changing vendor bank account information to their personal bank account
- Using agency credit cards and/or fuel cards for personal purchases
- Submitting reimbursements for expenses not incurred
- Using government assets for personal gain

Red flags

Employees who commit fraud often show certain behaviors—or red flags—that indicate they might be engaging in wrongdoing. While these red flags do not always mean that an employee is committing fraud, understanding and recognizing them can help your government more quickly detect fraud and mitigate any losses. For example, an employee who works long or odd hours and does not take sick leave or vacation may seem like a very dedicated public employee. However, that employee may also be taking advantage of business hours in which they are less likely to get caught committing fraud. Here are other behavioral red flags to be aware of:



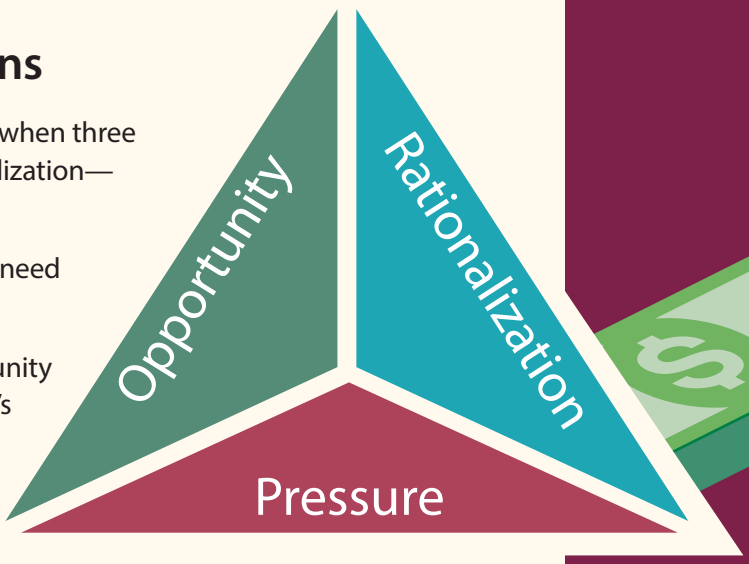
- Living beyond their means
- Experiencing financial difficulties
- Excessive control issues or unwillingness to share duties
- Unusually close relationship with a vendor or customer

The ACFE 2022 Report to the Nations concluded that at least one of these red flags appeared in 92 percent of fraud cases. The ACFE also estimates that the average organization loses 5 percent of its annual revenue to fraud each year, causing a median loss of $117,000 before it is detected.

SAO investigates frauds in all types of governments, from large state agencies to small special purpose districts. We have found that people in all types of positions at every level of government, from administrative assistants to department heads and elected officials, perpetrate fraud. On average, our office reports $3.8 million of public fund losses annually. No matter what type or size of government you oversee, fraud could happen to you.

How employee fraud happens

Usually, an employee chooses to commit fraud when three factors align: pressure, opportunity and rationalization—also known as the Fraud Triangle.



- **Pressure.** The employee has a motivation or need for money, often due to financial hardship.
- **Opportunity.** The employee has the opportunity to commit fraud because of the organization's poor internal controls. For example, a lack of segregation of duties allows an employee to commit and conceal the fraud at the same time.
- **Rationalization.** The employee convinces themselves that what they did was okay. For example, they rationalize that they deserve the additional compensation because they are underpaid and overworked.

An organization has little control over the pressures an employee may feel or the rationalizations they may make. To break the Fraud Triangle, governments instead must focus on reducing the opportunity for a fraud to occur.

Learn more

ACFE explains the Fraud Triangle in this short video

Preventing fraud

Your first line of defense in minimizing fraud risk is fraud prevention. Board members have a responsibility to develop an organization-wide framework that aims to prevent fraud. Here are tips to consider when designing your government's fraud-prevention framework:

- **Set the tone at the top.** A key responsibility of the board is to set the appropriate tone at the top through your attitudes, actions and communications. This tone helps define your agency's culture and influences the behavior of managers, employees, vendors, contractors and other stakeholders.
- **Set expectations for every employee as it relates to fraud.** Do not tolerate fraud at any level of the agency. Communicate this message—verbally and in writing—to all your employees. Ensure that management is encouraging ethical behavior and empowering employees, customers and vendors to insist that ethical standards are met every day.
- **Talk about fraud risks at your board meetings.** Have discussions at the board level about how fraud could occur, what internal controls your government has in place to prevent fraud, and how someone could override those controls.
- **Establish a fraud policy.** A well-crafted fraud policy is critical for communicating your agency's anti-fraud stance, the expected process for reporting fraudulent actions, and what happens to those who commit fraud. Your policy should focus on deterrence, detection, and correction of misconduct and dishonesty.
- **Be alert to the possibility of conflicts of interest.** It is not always possible to avoid conflicts of interest. Make sure that you identify and appropriately manage any potential, perceived or actual conflicts. For example, be aware of an employee—or even another board member—using their position to make financial decisions that result in an undisclosed personal gain.
- **Beware of the trusted employee syndrome.** The trusted employee syndrome occurs when boards and executives put full faith into someone and rely on their word because they trust them. It is great to have trusted employees in your agency, but you should also ask to see information from independent sources to verify their work, such as system-generated reports and actual bank statements. Remember: Trust is not an internal control.

Learn more

Sample fraud policies from

> Association of Certified Fraud Examiners

> The Fraud Advisory Panel

- **Attend meetings and interact with your external and internal auditors.** Do you understand the risks and issues auditors have identified relating to internal controls? SAO's auditors encourage board members to attend entrance and exit meetings for audits, and they will talk with you about risks your agency might encounter.
- **Perform a fraud risk assessment.** A risk assessment is a process for identifying your government's vulnerabilities to fraud and developing a plan to mitigate those risks before they cause damage. As board members, you can perform this assessment annually or hire a consultant to complete an independent assessment. Your insurance company may also provide this service for a small fee.

After you have completed your risk assessment, you will want to evaluate your government's insurance coverage for fraud loss. Make sure your agency has adequate coverage in the event a fraud occurs and that you regularly reassess whether it is enough. Also, take a close look at which employees you are bonding to minimize the agency's risk of misappropriation.

How to perform a risk assessment:

1. **Identify and document risks**
   Start with identifying fraud risks, which should include consideration of all types of schemes and scenarios, incentives, pressures and opportunities to commit fraud.

2. **Weigh the risks**
   Assess the relative likelihood of each fraud risk occurring. Interview staff and other key stakeholders to learn more about their roles.

3. **Mitigate the risks**
   Decide what the response should be to address the identified risks. You may want to conduct a cost-benefit analysis of fraud risks to help determine which controls or specific fraud-detection procedures to implement.

4. **Monitor the risks**
   Continually monitor the identified risks and conduct ongoing risk assessments to help mitigate them.

Keep in mind that executives and those higher up in management can cause the largest losses for an agency. Someone in your agency who is willing to steal likely knows the controls and operating procedures that are in place to prevent fraud—and they also know how to circumvent those controls and how to conceal their fraud. When evaluating the effectiveness of your controls, it is important to keep in mind the risk of management override.

Learn more

Watch this 6-minute video on how to conduct a fraud risk assessment.

Detecting fraud

You can never fully prevent fraud, so it is important to have a process for identifying fraudulent activities or attempts. As a board member, you are ultimately responsible for ensuring management fulfills its internal control responsibilities.

Too often, smaller organizations—those with fewer than 100 employees—rely on external auditors to detect fraud. Yet, when it comes to detecting fraud, auditors typically identify only about 5 percent of fraud cases. Auditors should not be viewed as a substitute for your board's own ongoing monitoring and development of policies and procedures.

Top five ways perpetrators conceal their fraud

Are you hesitant to review documents and ask staff too many questions? Here are the most common methods—according to the ACFE—that employees use to conceal their fraud, which underscore why your board should pay attention.

39% created fraudulent physical documents

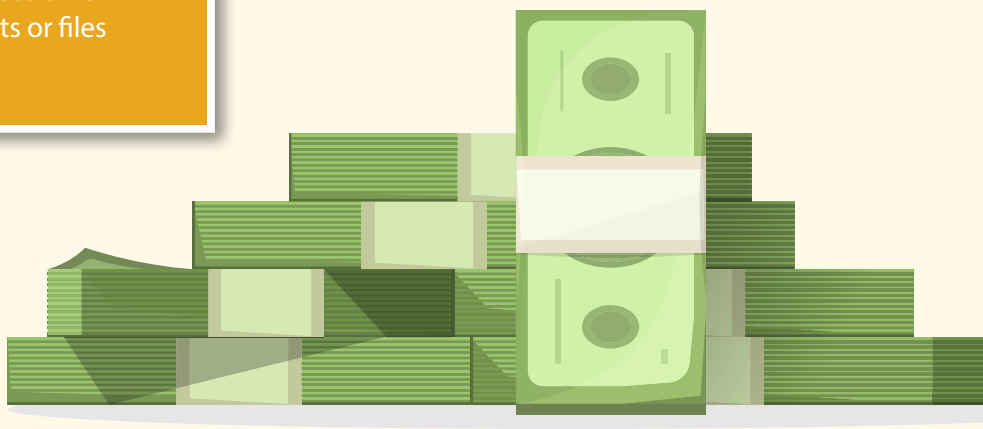
32% altered physical documents

28% created fraudulent electronic documents or files

25% altered electronic documents or files

23% destroyed or withheld physical documents

SAO's Segregation of Duties guide describes how to separate conflicting duty assignments to protect your government's assets. It covers all types of financial processes from cash receipting to payroll and banking. The guide also includes additional internal control options for small governments or small operations within larger governments.

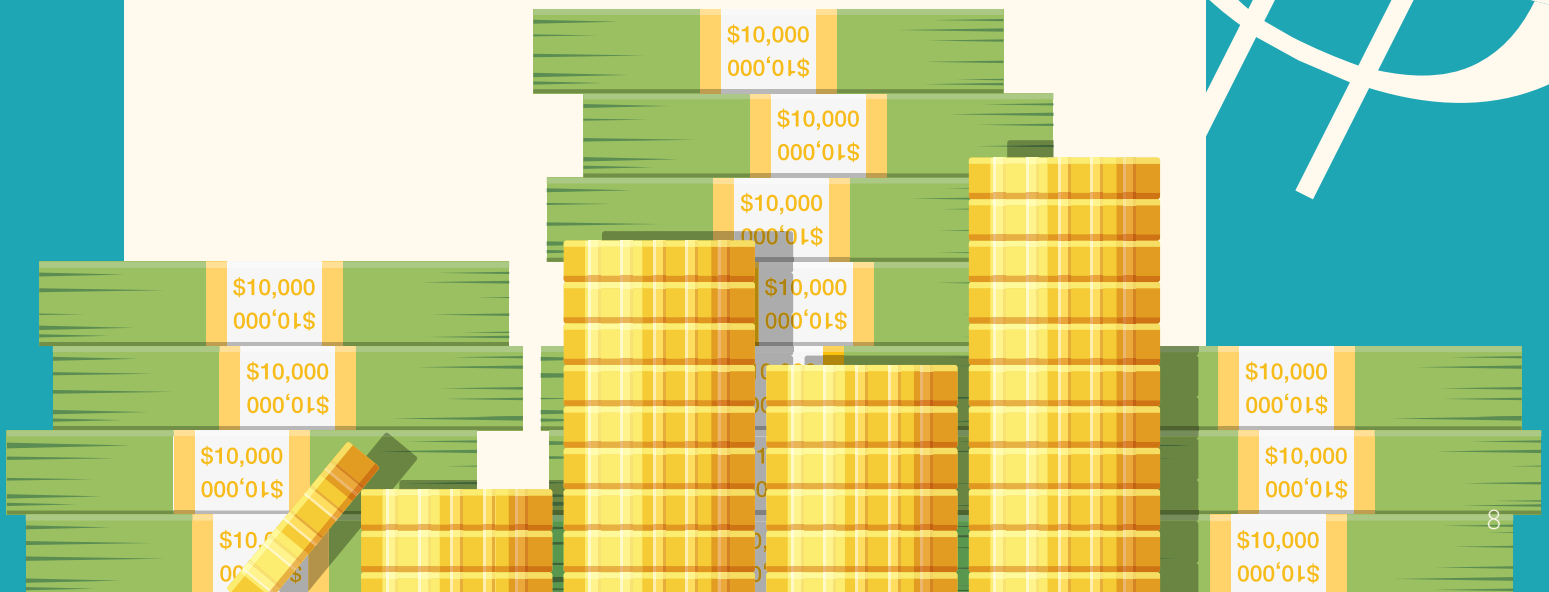


Here are tips for improving your board's ability to detect fraud:

- **Make sure your board is receiving accurate and timely financial information.** Most boards have fiscal responsibilities relating to budgeting or approving expenditures. For example, it is very important that you review actual documents and system-generated reports before approving expenditures.
- **Ask questions to ensure you understand what you are approving,** and make sure those answering your questions can provide adequate supporting documents.
- **Set up a tip hotline.** A tip hotline offers an anonymous way for people to report concerns via phone, mail or internet about suspected fraud. According to the ACFE, tips are the most common detection method by a significant margin—42 percent in the 2022 report—with more than half coming from employees and another 18 percent from customers. Many insurance companies or government risk pools may be able to help provide this service to your government at a very low cost. It is important to make sure that someone independent of operations, such as a board member, receives those tips.

If you do not know much about operations, consider first assessing your government's internal controls over financial reporting. This will help you understand how you can implement controls to mitigate risks. SAO has a self-assessment tool to help you get started.

On the next page, see SAO's list of the top three areas board members should review and monitor to detect fraud.



Three Simple Fraud Prevention & Detection Reviews

1

Review expenditures before you approve them

DO NOT accept verbal presentations or answers when approving expenditures.

DO

1. Review original documents and system-generated reports before approving expenditures.
2. Ask questions to make sure you understand all expenditures paid, which will help to confirm and verify expenses are for legitimate business purposes.
3. Make sure the staff answering your questions can provide adequate, original documents to support their statements.

2

The **truth** lies in the bank statements

DO NOT ignore your agency's bank statements or think you do not have enough time to review them.

A simple 15-minute scan of the transactions could help you detect unusual activity, especially if you review the statements each month and develop a baseline expectation of activity level and type.

DO

1. Make sure you know the source of the bank statements. Are they original, or are they copies that an employee could have altered before providing them for review?
2. Independently review the bank statements. If the employee misappropriating funds is the same person reviewing the bank statements and performing the reconciliation, the loss of funds could go undetected for years.
3. Take the time to understand how money comes in and goes out of your agency. Failure to review the bank statement might seem like a small oversight, but it could have drastic consequences. Bank account activity is the core source of a government's money flow in and out.

3

Pay **attention** to payroll

DO NOT accept verbal presentations or answers when approving payroll amounts. Employee compensation is typically one of the largest operating expenses for governments.

DO

1. Request a detailed payroll report that shows compensation paid to each employee.
2. Review employee compensation by types of compensation paid, such as salaried amounts, overtime, stipends or extra pay.
3. Ask questions to make sure you understand any compensation paid that is beyond the normal salaried amounts.
4. Make sure employee compensation agreements are documented and clearly defined. Consider annually comparing actual amounts paid to employment agreements to confirm that the amounts paid align with agreements.

Responding to fraud

If your government has not experienced an employee fraud yet, it likely will at some point. Moreover, when fraud is suspected or confirmed, it can be a chaotic time for your government. Being prepared to respond to a fraud event is critical to your government's response time, recovery and overall credibility.

Preparing for fraud before it happens

- **Develop a fraud response plan.** Having a fraud response plan to follow will help your board navigate through the crisis effectively and efficiently. The plan should include important steps to follow when addressing a fraud concern and help with identifying important details around the suspected or confirmed fraud. It should include how to handle notifying others who need to know, such as legal counsel, law enforcement and SAO.
- **Plan for negative public and media attention before it happens.** As part of your fraud response plan, designate a spokesperson for your agency and develop a process for handling media inquiries. Consider media training for your board, too.

The 10 Rs of Crisis Management is a good road map for designing a plan to respond, manage and recover from employee fraud.

Make sure to formally document your fraud response plan and incorporate it into your fraud policy.

What to do when you discover fraud

Washington state law (RCW 43.09.185) requires all state agencies and local governments to notify SAO immediately if staff suspects or knows that a loss of public resources or other illegal activity has occurred.

In the unfortunate event that your government is victim to fraud, we recommend you take the following actions:

- Follow your fraud response plan.
- Report the loss to SAO using the form on our website. Even if you do not have all the information yet, report the loss as soon as you can. You can always update a loss report when you have more information to share.

- Protect your agency's accounting records. Secure all original records related to the loss in a safe place until SAO has completed its investigation. For example, you should secure backup copies of computer records and original paper records related to the situation in a vault, safe or locked cabinet until the investigation is complete.
- Notify others who need to know. This may include other governing board members, department managers or financial officers, depending on the circumstances.
- Notify your legal counsel and file a police report with the local or state law enforcement agency, if appropriate.
- Do not enter into a restitution agreement with an employee before an investigation has established the amount of loss. Under state law (RCW 43.09.260), local governments must obtain written approval from SAO and the Attorney General's office before they make any restitution agreement, compromise, or settlement of loss claims covered by RCW 43.09.185.

Learn more

Questions about fraud? Contact SAO's Fraud Investigations Team at fraud@sao.wa.gov

Tips for responding to public and media attention

- **Act and respond quickly.** Designate a spokesperson (if you have not already). This can be an executive leader or an elected/appointed leader. Do your best to find someone who has had some media training.
- **Be transparent.** Try to have as many facts confirmed as possible before speaking publicly. Once you do speak publicly and you get a question that you do not have an answer to, it is okay to say that you do not have the information at the moment, but will find out.
- **Tell the truth the first time.** Make sure your facts are nailed down. Changing a series of facts after you have gone public with them breaks trust. If possible, tell the whole story at once. Try your best to avoid trickling out information.
- **Keep the audience as the focus.** Remember, reporters are trying to inform the same people you are. Do not argue with them. Ignore intentionally antagonistic people online. Do not block them, but do not engage with them either.

Additional resources

- Suspect a loss of public funds? This resource provides basic guidance on what to expect when working with SAO.
- SAO's Resource Library offers a variety of free guides, checklists and best practices to help Washington governments improve internal controls to prevent fraud.
- SAO's Preventing Fraud webpage contains multiple internal control assessment tools, guidebooks, free training links, and additional resources to help combat fraud.
- Bank statements deserve your attention. This article provides tips and best practices for what to look for when reviewing bank statements.
- Fraud Prevention Checklist – This checklist can help you test the effectiveness of your fraud prevention measures.
- The Association of Washington Cities (AWC) provides multiple educational resources and services for governments. Specific to risk management, we suggest looking at these pages:
  - > Risk Management Service Agency (wacities.org)
  - > Elected officials essentials workshop (wacities.org)
- The Municipal Research and Services Center (MRSC) provides good guidance on board responsibilities and practical tips for board members.

For assistance

This resource was developed by the Office of the Washington State Auditor. Please send any comments, questions, or suggestions to the Special Investigations Team at fraud@sao.wa.gov.

Disclaimer

This resource is provided for informational purposes only. It does not represent prescriptive guidance, legal advice, an audit recommendation, or audit assurance. It does not relieve governments of their responsibilities to assess risks, design appropriate controls, and make management decisions.

"Our vision is to increase **trust** in government. We are the public's window into how tax money is spent."

– Pat McCarthy, State Auditor

Washington State Auditor's Office
P.O. Box 40031 Olympia WA 98504

www.sao.wa.gov

1-564-999-0950

Office of the Washington State Auditor