



Payment Fraud Risks

Approving payments

Managers review and approve thousands of invoices, contractor statements, time sheets, expense reimbursements, purchase card details, and other payment vouchers every day. We encourage managers to answer some basic questions before approving invoices and other payments:

- Do you have firsthand knowledge that this vendor or contractor exists? If not, who can you contact to verify they do exist?
- Is this invoice based on an approved contract? Have the terms of the contract been met? If not, is a contract necessary based on the information in the invoice?
- Has the vendor/contractor provided the goods or services identified in the invoice or other billing statements? If you are not sure, verify with an independent source.

Are the correct amounts for price (including unit prices used), sales tax, freight and other variables addressed in the invoice?

- Are the prices being invoiced reasonable? Look for a standard
- to assess whether the price charged is reasonable.
- Do the quantities make sense? Do the quantities agree to the contract or agreement?
- Has anyone verified the invoice and other documents are mathematically correct?
- Has anyone verified this invoice has not already been paid?

Remember, it is appropriate to ask questions as part of the review process. Governments have a duty to ensure payments are supported and for a public purpose.

Fraud risks and controls

Governments should evaluate their risk of fraud on a regular basis. Fraud risks change as organizations change, so it is important to update assessment tools regularly.

Governments should consider several factors when assessing their fraud risk and the controls they have in place to mitigate fraud:

Our mission:

The State Auditor's Office holds state and local governments accountable for the use of public resources.

Reporting fraud online

The Washington State Auditor's Office has a tool for reporting suspected misappropriation online at:

www.sao.wa.gov



Identify potential risks and the associated costs.

- Identify your controls and assess the weaknesses within those processes
- Identify parties who could potentially take advantage of the risks and weaknesses.
- Identify the signs and signals (red flags) of fraud in your organization.
- Identify and access sources of information to detect fraud.
- Know your organization's standard data to identify possible red flags.
- Run tests and compare the results to your expected outcome.
- Evaluate, follow up and revise processes as necessary.

These steps have the potential to alert you to fraud, waste, or abuse within your organization. It is important to note that implementing these processes does not guarantee every occurrence of fraud will be caught or stopped.

What can you do?

Effective controls that prevent and detect fraud and abuse should be communicated to and are the responsibility of all employees. Some basic elements are:

- A basic understanding of red flags and remaining aware of the warning signs.
- Understanding how each employee fits into the organization's internal control structure. Knowing why processes and procedures exist helps employees understand why each step is important to protect against fraud, waste and abuse.
- Reading and understanding policies and procedures and being aware of changes.
- Reporting suspicious activity and inconsistencies that could be the result of fraud, waste, or abuse.

Did you know?

Over the past few months, our Office has received several reports of loss resulting from breaking and entering. For instance, small and attractive items such as laptops and digital cameras have been stolen out of government offices and employees' vehicles. This type of loss often can be prevented by instituting policies and procedures that require employees to lock items in the trunk or obscure them from sight.

Questions or comments

Sarah Walker

Fraud Manager

(509) 454-3621

[sarah.walker@sao.](mailto:sarah.walker@sao.wa.gov)

wa.gov