# Segregation of Duties

## Essential Internal Controls

Brought to you by the Center for Government Innovation, a service of the Office of the Washington State Auditor

Second edition, March 2026

Center for Government Innovation

# SIX GOLDEN RULES

## to Help Protect Your Government's Assets

1. Separate conflicting duties whenever you can, given your current staffing levels.

2. When you can't segregate duties, establish properly designed compensating controls to mitigate key areas of risk.

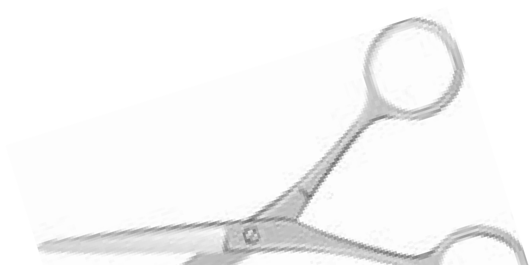
3. Document the controls you put in place, including duties you intend to segregate and other key controls, and include them in policy so that you communicate clear expectations to employees and management.

4. Incorporate consistent and effective supervision to ensure the controls you put in place are the correct ones and continue to operate effectively.

5. Use the security features in your software applications to enforce segregation of duties, such as by establishing user roles/permissions or workflows.

6. Review and reevaluate the internal controls you put in place periodically, especially during times of change. For example: When you adopt new software, staffing levels change or employee job duties change.

# Table of Contents



## 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.

SECTION 1

# Separating conflicting duty assignments can help protect your local government's assets

## Every government in Washington, no matter how broad or narrow its responsibilities, has a primary duty to safeguard the resources entrusted to it.

As straightforward as this directive sounds, small local government organizations – those with less than 20 or even 10 employees – struggle to meet this expectation. Why? Because with limited people to both do the work and provide oversight, these small governments may find themselves caught in a trap of incompatible job responsibilities. And when the same person takes in a customer's cash payment, writes out the deposit ticket, walks it to the bank and balances the bank statement at month's end, the opportunities for undetected error, fraud or theft increase. Just ask the State Auditor's Office. We have plenty of examples in our files, and we don't want your local government to be one of them.

We assume a local government's management and its governing body will work in harmony, so we mean both parties when we refer to "you" throughout this guide.

While larger governments may find it easier to segregate duties because they have more staff, they can struggle too. For example, a large county may have a small department accepting customer payments. Or they may allow the same employee to perform multiple conflicting duties because that is how it has been done for years, without realizing the risk of doing so. Like their smaller counterparts, large governments may also lack knowledge about which duties they should segregate – especially in their decentralized departments.

The principle of distributing these and similar tasks between different people is called a separation or segregation of duties. The separation of conflicting duties can reduce certain risks associated with financial processes and can help prevent and detect errors, fraudulent activity and in some cases, noncompliance with laws and regulations. It is a best practice for all local governments to follow as best they can with current staffing.

This guide, issued by the Office of the Washington State Auditor, offers all governments information about which duties to segregate for each financial process. And for those governments that cannot segregate some duties, it also provides potential compensating controls you can put in place to help mitigate risks related to conflicting duties.

## What's in this guide

There are entire books devoted to issues in accounting controls. This guide will not attempt to describe all the controls that you should have in place for various financial systems. It will cover:

- Overarching controls with broad benefits that support and enhance any specific controls you decide to put in place
- Duties you should segregate, given certain roles for a specific financial process
- Identification of the particular risks associated with specific incompatible duty assignments
- Control options to help minimize the risk when you can't separate conflicting duties (we call these compensating controls, and they usually involve some type of monitoring or oversight)
- Best practices for using technology to enforce segregation of duties
- Example strategies you might use to assign tasks and responsibilities when you have only one, two or three accounting employees
- Where to find a checklist, to help you quickly identify duties that you have not separated

## Basic concepts

Separating duties involves assigning responsibilities to different employees so that you can reduce your risk of error, fraud, theft or even noncompliance. When you cannot feasibly segregate duties, you must rely on controls that compensate for the heightened risk – usually that involves some form of additional monitoring and managerial oversight. Because you have many ways to attain effective internal control, the specific controls in place may look very different from one government to another.

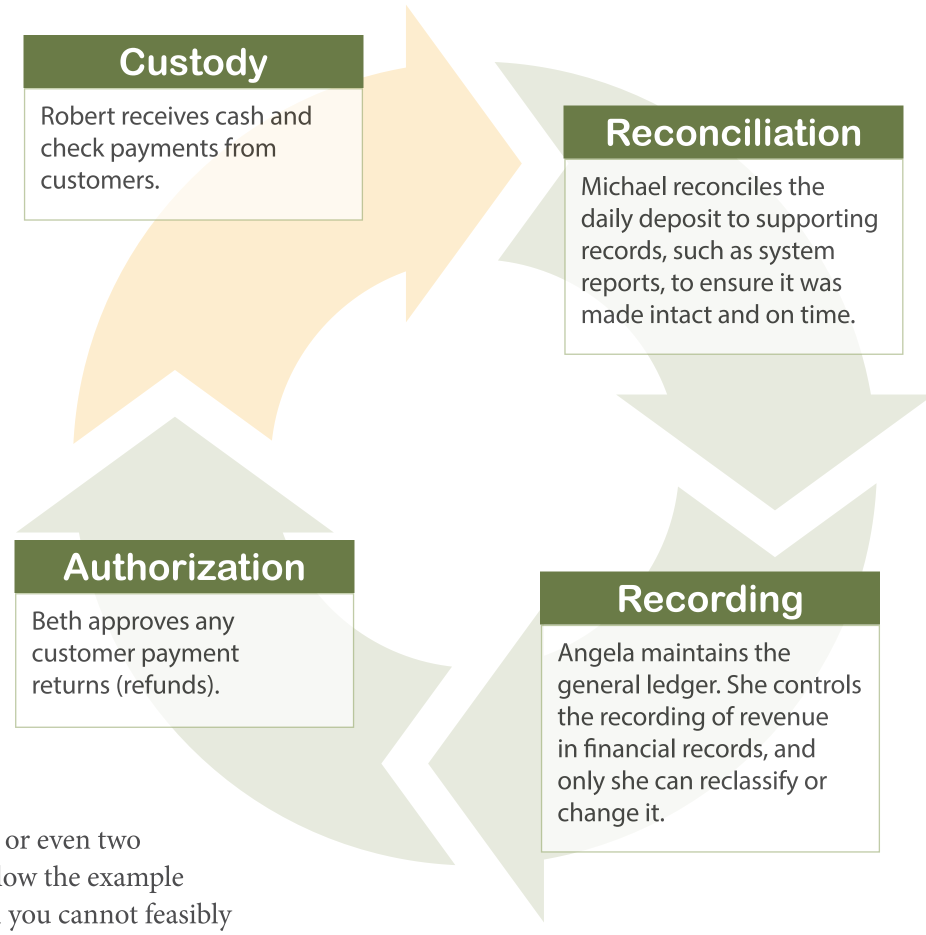
The State Auditor's Office doesn't prescribe how you should structure internal controls, but when we audit your government, we consider whether the internal controls you have put in place provide reasonable assurance you will meet your compliance and financial reporting objectives and adequately safeguard public assets. A local government's internal control system is management's responsibility, and so you must prepare to show your auditor and any other potential interested third parties that you have designed it well.

## An example of well-separated responsibilities

The duties associated with a cash receipting operation is a perfect example of tasks that different people should perform. **Diagram 1** shows how management has separated the roles of accepting customer payments (custody of assets), recording the revenue in the accounting records (recording), ensuring the deposit has been made correctly (reconciliation), and approving any reversal of customer payments such as refunds (authorization).

As you see, Robert may handle cash and other customer payments, but he can't adjust entries in the general ledger or accounting records, nor check his own work by reconciling the daily deposit. He also cannot authorize payment returns to customers in the form of refunds. Michael, Angela and Beth do not have access to customer payments. Separating duties like this helps reduce the risk of theft and errors because no one employee has too much control over a process. You may find identifying conflicting duties challenging, but typically they follow the custody, recording, reconciliation and authorization framework shown here.

**Diagram 1** – Separation of cash receipting roles




Some small cash receipting operations, such as those with only one or even two employees, will find it impossible to follow the example detailed above. In those instances when you cannot feasibly segregate duties due to limited staffing, the independent reviewer must play a bigger role as they attempt to "compensate" for the weakness within the control system. The independent reviewer must understand the risks created by the failure to segregate duties: the "what could go wrong." Then, they should practice additional oversight and monitoring with the specific risks in mind, so that they can detect errors, fraud/theft or possibly noncompliance.

Within your government, consider an employee who is "independent" with respect to accessing or handling money, an important consideration when that employee is performing certain tasks such as reconciling the deposit. An independent reviewer can identify and report discrepancies, such as a missing deposit, without anyone implicating them in the misappropriation. For independent oversight within very small governments, you might turn to one of your government's elected officials or a neighboring community you can swap oversight services with. If the budget allows, consider hiring an outside accountant to provide periodic reviews.

The next few pages list some general changes you can make to your government's expectations, policies and procedures to help improve internal controls and reduce overall risk. In Section 2, we describe the specific duties you should segregate for various financial processes and management of federal awards. We also describe the risks posed when your employees carry out conflicting duties, as well as potential compensating controls you might put in place to reduce the risks. Section 3 discusses how you should use technology within software applications to enforce segregation of duties. Appendix A sets out some strategies for small governments with one, two or three office employees to demonstrate how you might assign duties to reduce risk, as well as provide oversight for a small government. Finally, Appendix B will show you how to access a detailed checklist to help you assess where your government stands.

Don't wait for the State Auditor's Office to arrive to start work on these important financial safeguards.

## Overarching strategies that can have far-reaching effects

Attention to detail is important, but without attention to the big picture, individual actions can lack the context needed to have a meaningful effect. Here are some ideas that can deliver an extensive effect on the control structures of your local government. Some need only minimal resources to put in place.

**Begin by reflecting on the tone you want to set from the top of your government.**

As elected officials, executives, and department managers, consider the standards you want to guide your employees' behavior, as well as your own. These standards can then become your policies. Policies should incorporate actions and procedures, and where necessary, detail the consequences of employees failing to follow them.

### The ideal local government leadership team is:

#### Active

Review financial activity regularly. Ask questions about transactions that don't look quite right – and insist on seeing original supporting documents. Participate in the audit process: discuss issues and risks, and make sure you understand the audit results – especially if the auditor identifies possible or actual problems or concerns. Make sure that you or your employees follow up and resolve audit recommendations promptly.

#### Responsible

Develop and use financial forecasting and budgeting tools that include strong controls to limit spending. Set expectations around financial activity and establish a monitoring mechanism on a line-item basis. Follow up on significant variances.

### Observant

Get to know your employees. Pay attention to changes in lifestyle or financial pressures. Watch for red flags in behavior, such as employees who work late or on weekends, or resist changes to workplace practices. Address even small concerns or complaints brought to you by others, whether customers, colleagues or staff. They can reveal larger issues once investigated.

### Communicative

Make sure every employee knows your government's expectations concerning accountability and ethical behavior. Lead by example and hold yourself and others accountable to your expectations.

**Having established the standards you want employees to follow and embrace, formalize them in policies.**

This is so that all employees may understand and refer to them as questions arise. Policies around financial and accountability practices might address:

- *Fraud prevention.* Board members have a responsibility to develop a government-wide framework that aims to prevent fraud. SAO offers the "Trust but Verify" resource to help educate board members, which provides links to sample fraud policies.
- *Ethical behavior/conflicts of interest*. Items to consider include reporting and addressing conflicts of interest. Include ethical expectations of employees in policy, such as cash receipting, travel or any other policy addressing how employees should carry out financial transactions when conducting government business.
- *Whistleblower protection/tip hotline*. Consider how employees, or others external to the government, will share concerns. Employees may need a safe setting and certain assurances to come forward. You might refer to SAO's "Making It Easy to Report Concerns" resource as you work to implement this.
- *Background checks/bonding*. Require mandatory background checks and/or bonding, at least for certain positions.
- *Vacation leave*. Set and enforce mandatory annual leave for fiscal staff at all levels. Prohibit the holding of work for absent employees. Someone else should step in and perform the absent employee's duties - the employee filling in may detect irregularities that uncover larger issues.
- *Risk assessment*. Establish how and when management/leadership should perform risk assessments that encompass internal control systems, software applications, federal program compliance, financial reporting, fraud risks, along with other enterprise risks. We currently offer risk assessment tools for both GAAP financial reporting and federal program compliance.
- *Audits and other internal reviews*. An audit culture helps to ensure accountability for strong internal controls and compliant processes. Establish how you will practice such reviews in your government, and how you will engage with your external auditor.

**Follow through after policy development, with sensible practices and actions.**

Among the many elements that might arise as you plan and write policies, consider these first to reduce financial risk.

**Training.**

- Make sure employees understand your policies and how your internal control systems work and can recognize the symptoms of fraud. Make sure they know how and when to report concerns or "red flags" to management.

- Cross-train employees in each other's tasks, so you can periodically rotate assignments and responsibilities. This allows employees to periodically review each other's work, and in doing so, detect concerns.

**Plan financial reviews.**

- If a government does only one financial review, then you should read the bank statements. Our Office has investigated many losses of public funds that could have been detected sooner if only someone had looked at the bank statements. Our "Follow the Money" resource can help you make this task routine and simple.
- Schedule regular management review of financial reports, such as exception reports targeted at specific risks. For example, one such report might flag transactions posted in the system outside of regular work hours.
- Review revenue and expense trends for any unusual fluctuations, or deviations from budget, and follow up on them as appropriate.
- Periodically conduct unannounced spot checks or ask for supporting documentation, so employees know management is paying attention.

**Outsource duties.**

The practice of outsourcing duties can relieve considerable pain at the pinch-points of conflicting responsibilities. Among possible options:

- Use your county auditor, if they offer expenditure or payroll processing services in your area
- Use an outside service provider, such as a payroll service provider or a bank lockbox that accepts and processes mailed payments
- Use an outside accountant "contractor" to perform certain monitoring activities, such as completing bank account reconciliations
- Contract with another government, perhaps as a trade, to provide independent oversight for each other

SECTION 2

# Ten specific areas that need close attention

Each numbered chapter follows the same pattern. First, we describe the tasks, duties and responsibilities associated with a key role within different monetary areas of a typical local government. The following diagram shows that key role's relationship to others, whose duties should be segregated from their own. The key role is highlighted. Finally, a table with three columns sets out related but conflicting responsibilities the employee's government might assign them:

- The first column lists the conflicting duties or tasks.
- The second column lists some of the risks that arise when the same person is assigned the secondary duty or responsibility in addition to their main role.
- The third column offers some potential actions you can take to reduce the related risks, if you cannot segregate the duties.

Ideally, your local government looks just like the diagram on page 7, with enough staff to eliminate conflicting job duties. But we also recognize some governments may find this impractical or impossible for all their financial processes and may have some employees with conflicting responsibilities. That's where the suggested compensating controls in the third column come into action, as you should adopt such controls in these instances. It might take one or possibly a combination of several controls, carefully chosen using your best judgment or the advice of an accounting professional, to effectively reduce risk.

Even if you can't eliminate the risk entirely, when used effectively, these compensating controls can help reduce risk to an acceptable level.

# Cash receipting

Handling inbound cash and checks – for example, taking payment for water bills or property taxes – is one of the most common functions in local government accounting. This role is shown in the orange box in **Diagram 2**. It is separate from other roles' functions such as preparing customer billings, posting payments to customer accounts or overseeing the deposit (reconciliation controls).

**Diagram 2** – Cash receipting roles


**Table 1 –** Employee who receives payments and produces receipts for customers, or has other access to cash or checks for deposit:

| Roles this employee should not have | Risk if the employee has both roles | Compensating controls to consider |
|---|---|---|
| **Issuing receipts without supervision** | **Skimming schemes.** When an employee accepts money and issues receipts without supervision, they might misappropriate the cash or check and skip issuing a receipt to the customer (so that there is no record of the payment).<br><br>The employee may even use an unauthorized "manual" receipt book to issue fake receipts to customers, to hide the funds that they take.<br><br>**Note:** If you expect the cash receipts, as is the case with utility billings, then you have less risk of an employee "skimming" your payments and concealing the theft. However, even in these settings, governments usually have some unexpected or miscellaneous revenues at risk. | • Place surveillance cameras on receipting operations<br>• Place signs telling customers to expect a receipt, and urging them to contact a manager if they have concerns<br>• Use cash drawers that capture zero receipts (when the employee opens the drawer but does not record a transaction)<br>• Monitor the daily deposit for reasonableness, in total and amount of cash<br>• Conduct surprise cash counts, and look for unauthorized receipt books during the count<br>• Put additional controls in place to monitor infrequent and unexpected revenue streams<br>• Conduct an internal audit test: Have an auditor pose as a customer, pay in cash and not ask for a receipt. Assess whether the cashier properly recorded the funds and observe if the cashier insisted on providing a receipt.<br>• Monitor inventory for unexplained shortages |
| **Void receipts or issue refunds** | **Reversing transaction schemes.** When an employee accesses payments and can also void receipts or issue refunds, that employee might misappropriate money and conceal the theft by voiding a receipt or issuing a fake refund. | • Require cashiers to document all voids or refunds and account for them in the daily reconciliation. Periodically review void or refund activity for reasonableness.<br>• Require management approval for voids or refunds above a certain dollar amount<br>• Use software that maintains a proper audit trail of voided or cancelled receipts |

**Table 1 –** Employee who receives payments and produce receipts for customers, or has other access to cash or checks for deposit:

| Roles this employee should not have | Risk if the employee has both roles | Compensating controls to consider |
|---|---|---|
| **Accept cash and admit entry (such as into an event)** | **Skimming scheme.** The cashier can allow entry without giving the customer a ticket. This means there is no record of the transaction. They can then skim some of the cash received without anyone knowing. | • Whenever possible, do not hold ticketless events<br>• Post a sign telling customers to expect a receipt or numbered ticket, and to tell a manager if they don't get one. Then, reconcile the prenumbered tickets to revenue collected.<br>• Check that revenue generated meets expectations<br>• Perform surprise cash counts<br>• Compare an estimate of event attendees to revenue recorded, or use an actual figure if you have the means to obtain it |
| **Opening payments received in the mail** | **Check for cash substitution schemes.** This involves substituting a check, such as an unexpected payment that came in the mail, for cash that the employee collected and recorded earlier.<br>**Stolen check schemes.** This involves stealing checks and depositing them into a bank account the employee controls. | One way to uphold segregation of duties is to use a third party that has the desired controls, such as a bank lockbox service, for payment processing. Otherwise, consider these possible compensating controls:<br>• Require the employee to open mail, endorse checks and prepare the deposit in a supervised area<br>• Require daily deposit of all cash and checks (the longer they sit, the more opportunity an employee has to tamper with them)<br>• Place surveillance cameras where employees open mail<br>• Put additional controls in place to monitor infrequent and unexpected revenue streams<br>• Compare bank-validated deposit receipts to cash-receipting system reports to confirm the deposit's cash/check composition agrees with what cashiers received and recorded in the system |
| **Perform inventory adjustments (if accepting payment for inventoried goods)** | **Helps conceal a skimming scheme.** When the cashier can also adjust inventory, it becomes easier to hide skimmed payments for goods that they sold without recording the sale. | • Require documentation and management approval for inventory adjustments<br>• Periodically review inventory adjustments for reasonableness and the presence of supporting documentation<br>***See also the section on issuing receipts without supervision on page 13 (the compensating controls also focus on skimming schemes) |

**Table 1 –** Employee who receives payments and produce receipts for customers, or has other access to cash or checks for deposit:

| Roles this employee should not have | Risk if the employee has both roles | Compensating controls to consider |
|---|---|---|
| **Bill for goods or services** | **Over-billing schemes.** A clerk modifies the customer's invoice so that it demands more than the customer actually owes. Then, the employee misappropriates the over-payment when it arrives. | • Periodically trace transactions through the accounting system from origination to billing to payment as a spot check<br>• Periodically review billings before your employee mails them and look for potential alterations<br>• Independently send customers a separate statement, asking them to call management directly with questions about their account activity<br>• Monitor active accounts to ensure the employee correctly bills for services rendered |
| **Adjust customer accounts** | **Write-off schemes.** When the cashier can also adjust the customer's account to reduce the apparent amount owed, it becomes easier to conceal a stolen payment. | • Require supporting documentation for all customer account adjustments<br>• Require secondary authorization for adjustments, or at least for those exceeding a certain dollar amount<br>• Periodically review customer account adjustments for reasonableness, validity and for the presence of supporting documentation<br>• Independently send customers a separate statement, asking them to call management directly with questions about their account activity |

**Table 1 –** Employee who receives payments and produce receipts for customers, or has other access to cash or checks for deposit:

| Roles this employee should not have | Risk if the employee has both roles | Compensating controls to consider |
|---|---|---|
| **Applying payments to customer accounts** | **Lapping schemes.** These involve stealing Customer A's payment, and concealing the theft by applying Customer B's payment to Customer A's account.<br><br>**Over-posting schemes.** When the cashier can also mark accounts as paid, they could conceal stolen deposits by recording more payments than received. | **Particularly for lapping schemes:**<br>• Periodically spot-check how the employee applied customer payments to customer accounts, and compare payment date to the account posting date<br>• Monitor employees regularly working late hours or not taking vacations (lapping schemes take extra time to manage)<br>• Require daily balancing of all deposits, including mode of payment, to cash-receipting system reports or other source records and monitor this occurs<br>• Adopt, monitor and enforce a collection policy<br>• Monitor accounts receivable aging reports for changes (with lapping schemes, more accounts will show past-due)<br>• Independently send customers a separate statement, asking them to call management directly with questions about their account activity<br>**Particularly for over-posting schemes:**<br>• Reconcile total deposited to the total posted to customer accounts |
| **Preparing the deposit** | **Borrowing schemes.** A clerk who both accepts cash and prepares the deposit can substitute a personal check or a check from a later deposit for "borrowed" cash.<br><br>A clerk may also delay making the deposit, and temporarily "borrow" the cash for personal purposes. | • Periodically arrange for someone else to review the deposit before it goes to the bank to ensure cash/check composition agrees to the cash-receipting system reports or other source records.<br>• Ask the bank to periodically return the entire deposit for review and analysis by management, then verify the cash/check composition<br>• Monitor that the employee makes deposits daily, or as per your approved schedule (more frequent deposits give them less time and opportunity to tamper with it)<br>• Conduct a surprise cash count to look for personal checks in the deposit or missing funds |

**Table 1 –** Employee who receives payments and produce receipts for customers, or has other access to cash or checks for deposit:

| Roles this employee should not have | Risk if the employee has both roles | Compensating controls to consider |
|---|---|---|
| **Taking the deposit to the bank** | **Stolen deposit.** A clerk who both accepts money and takes the deposit to the bank can more easily steal part or all of the deposit.<br><br>**Delayed deposit.** When the same employee controls receipting and taking the deposit to the bank, they may choose to delay making the deposit to tamper with it. Then, they may carry out check-for-cash substitutions and borrowing schemes. | • Independently reconcile the deposit to the cash receipting system reports or other source records<br>• Establish a policy that sets out the frequency of deposits. State law (RCW 43.09.240) calls for deposit within 24 hours of receiving the money. You can apply for a waiver from your designated treasurer allowing up to one week, but you must comply with the 24-hour rule until you receive the waiver.<br>• Monitor to ensure the employee deposits the money daily or as expected per your authorized schedule<br>• Ask the bank for a validated receipt with cash and check components to help monitoring efforts |
| **Reconcile deposit source records to validated bank receipts** | **Stolen deposit,** in part or in full | **Note:** We strongly advise local governments not to give both these roles to the same person (one should never audit themselves)<br>• If it is unavoidable, at a minimum an independent person should periodically review the reconciliation to ensure the employee made each deposit intact and on time as per your authorized schedule<br>• Monitor deposit totals over time, to ensure reasonableness. Use historical data to develop expectations for deposit totals to detect variances. |
| **Reconcile the bank statement** | **Stolen deposit,** in part or in full | **Note:** We strongly advise local governments not to give both these roles to the same person. To uphold segregation of duties, you might consider outsourcing the bank reconciliation to a contracted accountant. Otherwise consider these possible compensating controls:<br>• Monitor deposit activity using online banking access and deposit source records (or request a mailed statement copy from the bank) |

**Table 1 –** Employee who receives payments and produce receipts for customers, or has other access to cash or checks for deposit:

| Roles this employee should not have | Risk if the employee has both roles | Compensating controls to consider |
|---|---|---|
| | | • Perform a secondary review of the bank reconciliation<br>• Periodically have an independent person re-perform the reconciliation in its entirety<br>• Monitor revenue streams for reasonableness |
| **Participate in accounts payable functions** | **Shorted deposit concealed with accounts payable check.** A clerk with the ability to write checks AND receive cash can issue government checks to back-fill shorted deposits that they stole. In other words, the employee can withdraw cash from the deposit and substitute the government's own check for the stolen cash. | • Thoroughly review accounts payable payments, especially checks made out to the government's own name<br>• Periodically review the composition of a deposit right before it is taken to the bank. For example, look for checks that are not from customers.<br>• Check the deposit records to ensure cash/check composition agrees to the cash-receipting system records |
| **Prepare journal entries, or otherwise modify the general ledger** | When the same employee has access to money and can also make journal entries, they may move funds within the general ledger to conceal theft or loss of funds. | • Require secondary review of each journal entry and its supporting documentation. Be alert to journal entries directly affecting cash or reclassifications of revenue.<br>• Periodically review for and follow up on unusual journal entries |

# Accounts receivable

Accounts receivable oversees customer accounts and activity, posts payments, and performs collection efforts to collect on past due amounts for services rendered, such as utility services. This role is shown in the orange box in **Diagram 3**. It is separate from other functions such as roles that receipt cash, generate billings or process customer refunds.

**Diagram 3** – Accounts receivable roles

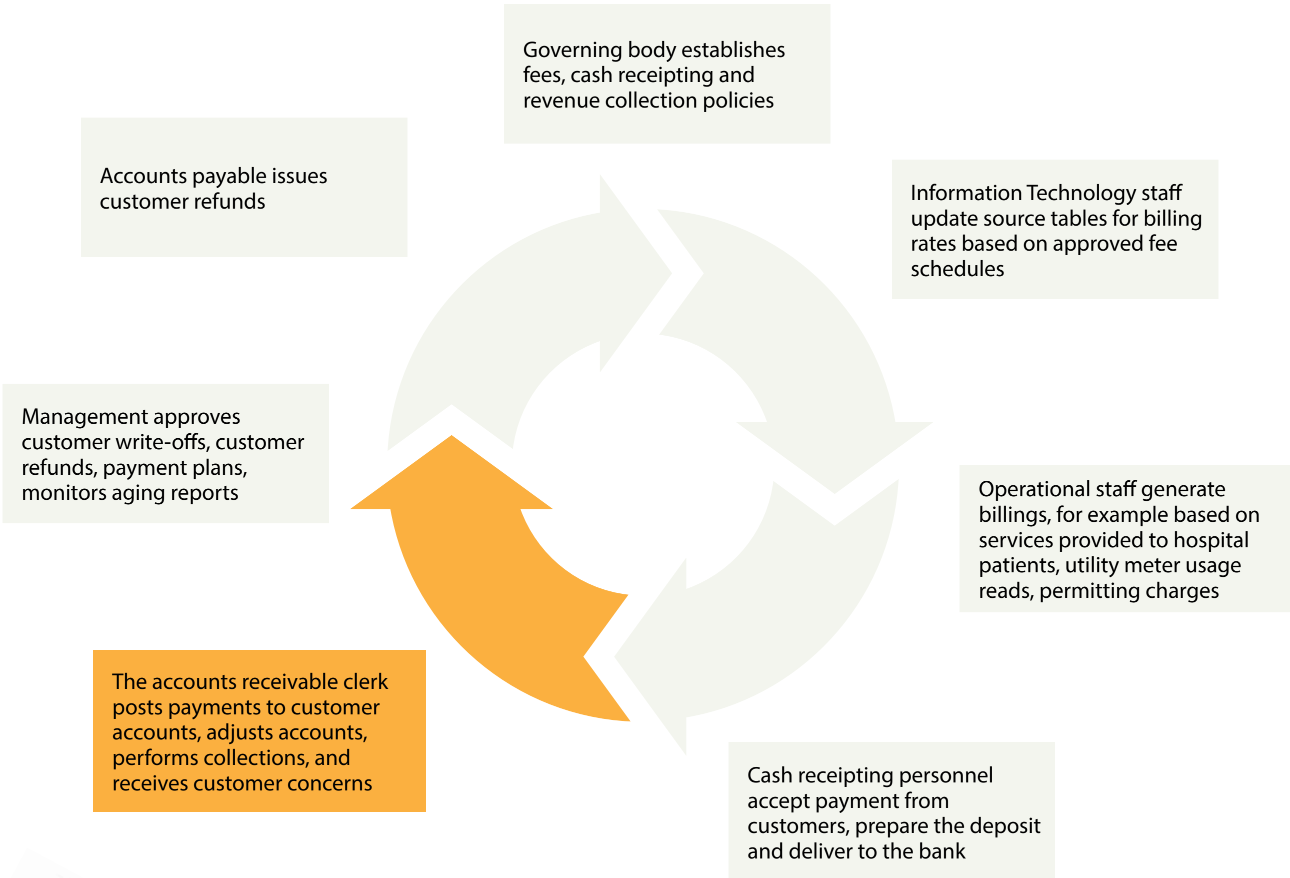



**Table 2 –** Employee who handles customer accounts and collections as accounts receivable:

| Roles this employee should not have | Risk if the employee has both roles | Compensating controls to consider |
|---|---|---|
| **Have or take custody of cash or checks, including:**<br>• Acting as a primary or backup cashier<br>• Handling or having access to deposits<br>• Having access to mailed payments, including nonroutine payments such as those received from collection agencies | **Lapping schemes**. These involve stealing Customer A's payment, and concealing the theft by applying Customer B's payment to Customer A's account.<br>**Over-posting schemes.** When the cashier can also mark customer accounts as paid, they could conceal stolen deposits by recording more payments than received.<br>**Write-off schemes.** When the cashier can also adjust the customer's account to reduce the apparent amount owed, it becomes easier to conceal a stolen payment.<br>Refer to Chapter 1: Cash Receipting, for more information. You may have more additional risks than described here, depending on duty assignments. | **Particularly for lapping schemes:**<br>• Periodically spot-check how the employee applied customer payments to customer accounts and compare the payment date to the account posting date<br>• Monitor employees regularly working late hours or not taking vacations (lapping schemes take extra time to manage)<br>• Require daily balancing of all deposits, including mode of payment, to cash-receipting system reports or other source records, and monitor to ensure this occurs<br>• Adopt, monitor and enforce a collection policy<br>• Monitor accounts receivable aging reports for changes (more accounts will show past-due in the event of lapping schemes)<br>• Independently send customers a separate statement, asking them to call management directly with questions about their account activity<br>**Particularly for over-posting schemes:**<br>• Reconcile total deposited to the total posted to customer accounts<br>**Particularly for write-off schemes:**<br>• Require supporting documentation for all customer account adjustments<br>• Require secondary authorization for adjustments, or at least for those exceeding a certain dollar amount<br>• Periodically review customer account adjustments for reasonableness, validity and for the presence of supporting documentation<br>• Independently send customers a separate statement, asking them to call management directly with questions about their account activity |

**Table 2 –** Employee who handles customer accounts and collections as accounts receivable:

| Roles this employee should not have | Risk if the employee has both roles | Compensating controls to consider |
|---|---|---|
| Be responsible for managing the billing/invoicing system, including updating it for new billing rates and editing billings, and sending out invoices | **Billing errors.** If the accounts receivable clerk does not have access to customer payments or deposits, then the risk is limited to having too much control over the process, and that billing errors may occur and go undetected.<br><br>If your employee also receipts cash or otherwise accesses customer payments, refer to Chapter 1, Cash Receipting, for the related fraud risks for those two conflicting duties: cash receipting and billing. | • Periodically review invoices for accuracy before your employee mails them<br>• On a sample basis, agree rates and fees charged to ensure they agree to your approved board resolution<br>• Test one iteration of each possible billing scenario to ensure accuracy<br>• Ensure a second employee reviews changes made to billing rate tables within a software system<br>• Independently send customers a separate statement, asking them to call management directly with questions about their account activity |
| Authorize write-offs of customer accounts, customer credit memos or customer refunds | **Amounts owed to you may go uncollected.** If the accounts receivable clerk does not have access to customer payments or deposits, then the risk is limited to having too much control over the collections process. For example, they might write off accounts that they should have actively worked to collect.<br><br>If your employee also receipts cash or otherwise accesses customer payments, refer to Chapter 1, Cash Receipting, for the related fraud risks for those two conflicting duties: cash receipting and adjusting customer accounts. | • Adopt and enforce a collection policy that establishes expectations for the accounts receivable clerk<br>• Periodically monitor collection efforts to ensure employee actions to collect past due accounts comply with policy<br>• Require supporting documentation for all account write-offs, credits or refunds<br>• Require secondary approval for account write-offs, credits or refunds exceeding a certain threshold<br>• Periodically review account write-offs, credits or refunds for reasonableness, validity and the presence of supporting documentation |
| Approve payment plans | **Amounts owed to you may go uncollected.** This gives accounts receivable clerks too much control over the collections process. They might not follow the collections policy, such as by showing too much leniency to customers. | • Periodically review the customer accounts with payment plans to ensure they qualified for a payment plan, and that documentation supports it<br>• Monitor the number of customers with payment plans for unusual fluctuations |

# Payroll

The payroll clerk typically processes employee timesheets and generates payroll for a local government. This employee's position is shown in the orange box in **Diagram 4**. It is separate from other duties related to payroll processing, such as those duties that establish wage rates, approve payroll payments, and issue or distribute payroll checks.

**Diagram 4 –** Payroll roles

**Table 3 –** Employee processes payroll (typically called a payroll clerk):

| Roles this employee should not have | Risk if the employee has both roles | Compensating controls to consider |
|---|---|---|
| Edit the personnel master file, including the ability to add new employees, change wage rates or compensation, or change bank routing information for direct deposits. | **Falsify wage rates.** An employee could increase personal compensation for themself, friends or family.<br><br>**Create ghost employees.** An employee could create a fictitious (ghost) employee and use that record to divert money to a bank account they control. A related scheme converts a prior employee's record into a fake ongoing payee.<br><br>**Note:** You may have a higher risk of ghost employees if your software configuration allows the payroll clerk to also approve or process unapproved timesheets. | **For both schemes:**<br>• Review a monthly report of any changes made to wage rates or salary, employee names, addresses or bank routing information<br>• Periodically compare a report of employees and wage rates (per the payroll system) to employee files and other source records to verify employment status and pay rate<br><br>**Particularly for falsified wage rate schemes:**<br>• Review the final payroll register carefully, checking the wage rate/compensation of employees with the ability to make changes within the payroll system (as well as any familial relations, if applicable)<br><br>**Particularly for ghost employee schemes:**<br>• Review the final payroll register for unfamiliar names or separated employees receiving payment<br>• Investigate any "temporary or seasonal" employees who continue to receive payments after their expected separation date<br>• Periodically review employee addresses and bank account numbers to determine if multiple payments route to the same address or bank account. Verify requests to change a street address to a post office box.<br>• Require departmental managers to regularly review their employee payroll reports for anything unusual, and report concerns to management |
| Approve time sheets or process unapproved time sheets | **Falsify time worked.** Increasing personal compensation for self, friends, family or in collusion with another employee | • Review the final payroll register and closely monitor hours worked, for the payroll clerk and any related employees |

**Table 3 –** Employee processes payroll (typically called a payroll clerk):

| Roles this employee should not have | Risk if the employee has both roles | Compensating controls to consider |
|---|---|---|
| Serve as the auditing officer | **Execute unauthorized payments.** When the same employee can process payments and certify them as valid, they might conceal unauthorized payments | **Note:** We strongly advise local governments not to give both these roles to the same person. To uphold segregation of duties, you might consider transferring the oversight responsibilities of the auditing officer to someone else, such as an elected official or a contractor. Alternatively, you might outsource the payroll processing function to a third party. Otherwise, consider these possible compensating controls:<br>• Periodically log into the payroll system and monitor payroll activity, especially the payroll clerk's compensation. Run and review key reports to monitor payroll activity.<br>• Do not allow employees to process payroll payments before the governing body approves them. The governing body should play an active role and regularly ask for original support for select transactions. An independent person should monitor the banking activity for any payments that bypass board approval. |
| Generate payments or have access to checks | **Execute unauthorized payments**<br>**Check alteration schemes.** When the same employee responsible for producing payroll can also generate checks, they could alter the payee name or deposit checks directly into a personal account<br>**Electronic payment schemes.** A clerk who can access and edit the Automated Clearing House (ACH) | **Note:** We strongly advise local governments not to give both these roles to the same person. To uphold segregation of duties, you might consider outsourcing payroll payment generation. Otherwise, consider these possible compensating controls: |

**Table 3 –** Employee processes payroll (typically called a payroll clerk):

| Roles this employee should not have | Risk if the employee has both roles | Compensating controls to consider |
|---|---|---|
| | payment file can change banking information and redirect payments to their own bank account (the ACH payment file contains employee banking information and payment amounts and is submitted to the bank, so that the bank may carry out the "direct deposit"). | **Particularly for unauthorized payment schemes:**<br>• Verify that the payroll run, as approved by management, agrees in total to the actual payment amount (as per total checks issued, or total direct deposit as per the bank statement)<br>• Use a separate bank account, referred to as a clearing account. Use this only for payroll payments to limit the funds available. Also, reconcile this account.<br>• Use prenumbered check stock, and safeguard and track it<br>• Monitor for gaps in the check sequence<br>**Particularly for check alteration schemes:**<br>• Assign someone else to mail or distribute the checks<br>• Review endorsed payroll checks, preferably received directly from the bank, for alterations<br>• Consider using your bank's Positive Pay service (or reverse positive pay) to detect check alterations<br>**Particularly for electronic payment schemes:**<br>• Require a second person to review the ACH payment file and authorize the release of funds (you can set this up with your bank)<br>• Ensure your ACH payment file is read-only (no one can edit it)<br>• Periodically compare the bank's ACH receipt to your original source records, to ensure no one diverted funds to an unauthorized bank account (Note: the direct deposit withdrawal will show as one line item on your bank statement due to the bank's batching of ACH payments) |

**Table 3 –** Employee processes payroll (typically called a payroll clerk):

| Roles this employee should not have | Risk if the employee has both roles | Compensating controls to consider |
|---|---|---|
| Ability to authorize payroll payments in any form, including signing checks, approving electronic fund transfers or otherwise serving as a signer on any of the government's bank accounts | **Execute unauthorized payments** | **Note:** We strongly advise local governments not to give both these roles to the same person. To uphold segregation of duties, you might outsource the payroll processing function to a third party.<br>• If it is unavoidable, at a minimum, an independent person should periodically review bank account activity, using online access or by requesting a copy of the bank statement(s) directly from the bank. This independent person should perform a detailed review of payroll payment activity as reflected in the banking records and trace it to support.<br>• In addition, we advise that you prohibit the clerk from sending out payroll payments before the governing body reviews and approves them. The governing body should play an active role and regularly ask for original support for select transactions. An independent person should monitor the banking activity for payments that bypass board approval.<br>**If you pay vendors electronically:**<br>• Require a second person to review the ACH payment file and authorize the bank to release funds (you can set this up with your bank)<br>• Periodically compare the bank's ACH receipt to your original source records, to ensure no one diverted payroll funds to an unauthorized bank account (Note: the direct deposit withdrawal will show as one line item on your bank statement due to the bank's batching of payments)<br>**If you pay vendors by check:**<br>• Use two-signature authorizations on all checks. However, some banks will not monitor this and you will need to consider other controls. |

**Table 3 –** Employee processes payroll (typically called a payroll clerk):

| Roles this employee should not have | Risk if the employee has both roles | Compensating controls to consider |
|---|---|---|
| Reconcile the bank account or payroll clearing account | **Execute unauthorized payments.** When the same employee processes payroll and reconciles bank accounts, they could make and conceal unauthorized payments | **Note:** We strongly advise local governments not to give both these roles to the same person. To uphold segregation of duties, you might consider outsourcing the bank reconciliation to a contracted accountant. Otherwise consider these possible compensating controls:<br>• Monitor expenditure activity using online banking access and trace to source records (or have the bank mail you a copy of the statement)<br>• Perform a secondary review of the bank reconciliation<br>• Periodically have an independent person reperform the reconciliation in its entirety<br>• Monitor payroll check runs or electronic payment transactions closely, ensuring all activity is appropriate and reconciles to bank withdrawals |
| **Prepare journal entries, or otherwise modify the general ledger** | When the same employee can process payroll payments and make journal entries, they may move funds within the general ledger to conceal theft or loss of funds. | • Require secondary review of each journal entry and its supporting documentation. Be alert to journal entries directly affecting cash or reclassifications of expense.<br>• Periodically spot-check for unusual journal entries and follow up |

# Accounts payable

The accounts payable department typically processes all of a local government's payments to vendors. The accounts payable processor's role is shown in the orange box in **Diagram 5**.

It is separate from other functions such as roles that purchase those goods and services, record receipt of the goods and services, and that authorize payments.

**Diagram 5 –** Accounts payable roles

**Table 4 –** Employee processes vendor payments (typically as an accounts payable clerk):

| Roles this employee should not have | Risk if the employee has both roles | Compensating controls to consider |
|---|---|---|
| Create new vendors or make other changes to the vendor master file | **Fictitious vendor schemes.** An accounts payable clerk who can also create a new vendor can set up a fictitious payee using a personal address and/or bank account and direct payments to that account.<br><br>A variation redirects payments processed using a legitimate vendor record to the clerk's own address or bank account. | • Review a monthly report of all changes to vendor information<br>• Require management approval to set up new vendors or to make changes to existing vendors (the review should ensure each new vendor is legitimate)<br>• Periodically compare employee addresses, bank information and phone numbers to those of vendors<br>• Review vendor invoices with extra scrutiny<br>• Review reports of expected or scheduled payments and monitor for and follow up on any unfamiliar vendors<br>• Periodically evaluate that the vendor's efforts to carry out contracted work match expectations |
| Serve as the auditing officer | **Execute unauthorized payments.** When the same employee can process payments and certify them as valid, they could conceal unauthorized payments. | **Note:** We strongly advise local governments not to give both these roles to the same person. To uphold segregation of duties, you might consider transferring the oversight responsibilities of the auditing officer to someone else, such as an elected official or a contractor. Otherwise consider these possible compensating controls:<br>• Consider establishing a financial oversight subcommittee of the governing body to carefully review all payments before issuing them<br>• Do not allow staff to process payments before the governing body approves them. The governing body should play an active role and regularly ask for original support for select transactions. An independent person should monitor the banking activity for any payments that bypass board approval. |

**Table 4 –** Employee processes vendor payments (typically as an accounts payable clerk):

| Roles this employee should not have | Risk if the employee has both roles | Compensating controls to consider |
|---|---|---|
| Generate payments or have access to checks | **Execute unauthorized payments**<br><br>**Check alteration schemes.** An accounts payable clerk with access to checks could alter the payee name, or deposit the checks directly into a personal account.<br><br>**Electronic payment schemes.** A clerk who can access and edit the ACH payment file can change banking information and redirect payments to their own bank account (the ACH payment file contains vendor banking information and payment amounts and is submitted to the bank, so that the bank may carry out electronic payments). | **Note:** We strongly advise local governments not to give both these roles to the same person. To uphold segregation of duties, you might consider outsourcing payment generation. Otherwise consider these possible compensating controls:<br><br>**Particularly for unauthorized payment schemes:**<br>• Verify that the total payment amount generated agrees to what management authorized (in dollars)<br>• Use a separate bank account, referred to as a clearing account. Use this only for accounts payable payments to limit the funds available. Also reconcile this account.<br>• Use prenumbered check stock and safeguard and track it<br>• Monitor-for gaps in the check sequence<br><br>**Particularly for check alteration schemes:**<br>• Assign someone else to mail the checks (do not return them to accounts payable)<br>• Review endorsed checks, preferably received directly from the bank, for alterations or unauthorized payments<br>• Consider using your bank's Positive Pay service (or reverse positive pay) to detect check alterations<br><br>**Particularly for electronic payment schemes:**<br>• Require a second person review the ACH payment file and authorize the release of funds (you can set this up with your bank)<br>• Ensure your ACH payment file is read-only (no one can edit it)<br>• Periodically compare the bank's ACH receipt to your original source records, to ensure no one diverted funds to an unauthorized bank account (Note: the direct deposit withdrawal will show as one line item on your bank statement due to the bank's batching of ACH payments) |

**Table 4 –** Employee processes vendor payments (typically as an accounts payable clerk):

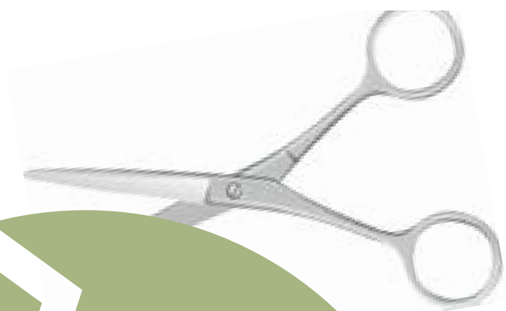
| Roles this employee should not have | Risk if the employee has both roles | Compensating controls to consider |
|---|---|---|
| Ability to authorize payments in any form, including signing checks, approving electronic funds transfers or wire transfers, or otherwise serving as a signer on the government's bank accounts | **Execute unauthorized payments** | **Note:** We strongly advise local governments not to give both these roles to the same person.<br>• If it is unavoidable, at a minimum an independent person should periodically review bank account activity, using online access or by requesting a copy of the bank statement(s) directly from the bank. This independent person should perform a detailed review of expenditure activity as reflected in the banking records and trace it to support.<br>• In addition, we advise that you prohibit the clerk from sending out payments until after the governing body reviews and approves them. The governing body should play an active role and regularly ask for original support for select transactions. An independent person should monitor the banking activity for payments that bypass board approval.<br>**If you pay vendors electronically:**<br>• Require a second person to review the ACH payment file and authorize the bank to release funds (you can set this up with your bank)<br>• Impose a wire limit with the bank for any authorized person<br>• Require your bank to obtain secondary authorization for wire transfers, or for those that exceed a certain threshold, or that are non-repetitive<br>• Periodically compare the bank's ACH receipt to your original source records, to ensure no one diverted funds to an unauthorized bank account (Note: the ACH payments will show as one line item on your bank statement due to the bank's batching of payments)<br>**If you pay vendors by check:**<br>• Use two-signature authorizations on all checks. However, some banks will not monitor this and you will need to consider other controls |

**Table 4 –** Employee processes vendor payments (typically as an accounts payable clerk):

| Roles this employee should not have | Risk if the employee has both roles | Compensating controls to consider |
|---|---|---|
| Reconcile the bank account or clearing account | **Execute unauthorized payments.** | **Note:** We strongly advise local governments not to give both these roles to the same person. To uphold segregation of duties, you might consider outsourcing the bank reconciliation to a contracted accountant. Otherwise consider these possible compensating controls:<br>• Monitor expenditure activity using online banking access and trace to source records (or have the bank mail you a copy of the statement)<br>• Perform a secondary review of the bank reconciliation<br>• Periodically have an independent person reperform the reconciliation in its entirety<br>• Monitor accounts payable check runs or electronic payment transactions closely, ensuring all activity is appropriate and reconciles to bank withdrawals |
| Participate in cash receipting functions | **Conceal a shorted deposit.** A clerk with the ability to process "check" payments AND receive cash, can issue government checks to back-fill shorted deposits that they stole. In other words, the employee can withdraw cash from the deposit and substitute the government's own check for the stolen cash. | • Thoroughly review accounts payable payments, especially checks made out to your government's name<br>• Periodically review the composition of a deposit right before it is taken to the bank<br>• Check the deposit records to ensure cash/check composition agrees to the cash-receipting system reports or other source records |

**Table 4 –** Employee processes vendor payments (typically as an accounts payable clerk):

| Roles this employee should not have | Risk if the employee has both roles | Compensating controls to consider |
|---|---|---|
| Procure goods or services | **Execute unauthorized payments / kickback schemes.** A clerk with the ability to procure from vendors and also process their invoices has too much control over the overall transaction. They may make personal purchases or pay inflated prices in exchange for "kickbacks" from the vendor. | **Note:** We strongly advise local governments not to give both these roles to the same person. Otherwise, consider these potential compensating controls:<br>• Review vendor payments with increased scrutiny<br>• Periodically verify goods purchased arrived on-site; monitor ship-to addresses<br>• Periodically evaluate that the vendor's efforts to carry out contracted work match expectations<br>• Evaluate pricing of goods and services for reasonableness, and monitor for significant price increases that appear unfavorable to the government |
| Prepare journal entries, or otherwise modify the general ledger | When the same employee can process payments, and can also make journal entries, they may move funds within the general ledger to conceal theft or loss of funds. | • Require secondary review of each journal entry and its supporting documentation. Be alert to journal entries directly affecting cash or reclassifications of expense<br>• Periodically spot-check for unusual journal entries and follow up |



# Purchasing and procurement

The procurement or purchasing department is usually responsible for vendor solicitation, buying and managing the process for acquiring goods and services. The procurement role is shown in the orange box in **Diagram 6**. The procurement role is separate from other roles, such as physically receiving the goods or processing payments to vendors. These three distinct roles also correlate to the three-way match that should occur and support all vendor payments – purchase order, receiving documents and vendor invoice.

**Diagram 6 –** Purchasing system roles

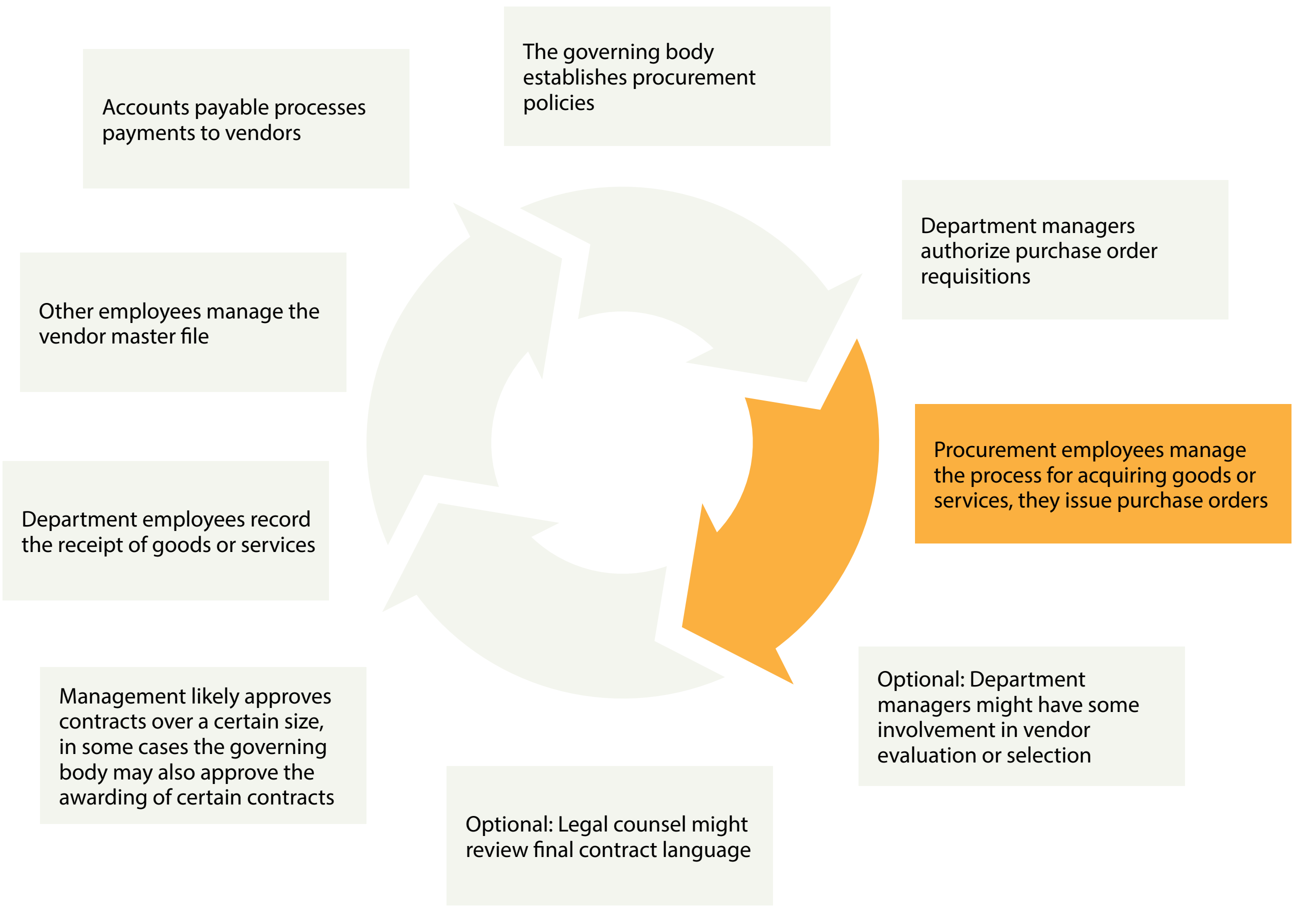


**Table 5 –** Employee purchases or procures goods and services from vendors:

| Roles this employee should not have | Risk if the employee has both roles | Compensating controls to consider |
|---|---|---|
| Negotiate contracts without oversight or involvement by other employees | **Kickback schemes.** An employee is bribed, or solicits vendors for bribes, in exchange for awarding a contract to a vendor, potentially without inviting competing bids or at unfavorable pricing. Bribes may include cash, gifts or other forms of enticement. | • Establish a procurement policy and require competitive processes, and sealed bid openings where appropriate<br>• Perform a secondary review of contracts, considering the selection process, terms and vendor performance<br>• Evaluate pricing of goods and services for reasonableness, and monitor for significant price increases that appear unfavorable to the government<br>• Establish a vendor code of ethics policy and share it with them, such as once a year or include it in bid packets for larger procurements. Ask vendors to report to you if any of your employees solicit bribes from them.<br>• Include a right-to-audit clause in your vendor contracts/purchase orders |
| Receive or take custody of the goods they procure | **Order-and-take schemes.** Employees purchase goods that they can then use for personal purposes, privately sell, or return for credits or gift cards. | • Perform a spot-check to ensure ordered goods arrived on-site<br>• Review purchase activity for reasonableness, including nature and frequency of purchases<br>• When approving payments, look for vendor invoices with unfamiliar "ship-to" addresses |

**Table 5 –** Employee purchases or procures goods and services from vendors:

| Roles this employee should not have | Risk if the employee has both roles | Compensating controls to consider |
|---|---|---|
| Create new vendors or make other changes to the vendor master file | **Fictitious vendor schemes.** A procurement employee who can also create a new vendor can set up a fictitious payee and issue a purchase order to them for goods or services that the government will never receive. The employee would later fabricate an invoice to complete the misappropriation.<br><br>Another variation of this scheme involves the employee establishing a separate business for purposes of reselling goods to their employer at inflated prices. | • Review a monthly report of all changes to vendor information<br>• Require management approval to set up new vendors or to make changes to existing vendors (the review should ensure each new vendor is legitimate).<br>• Periodically compare employee addresses, bank information, and phone numbers to those of vendors.<br>• Periodically evaluate that vendor's efforts to carry out contracted work matches expectations<br>• Review vendor payments with extra scrutiny<br>• Review reports of expected or scheduled payments, monitor for and follow up on any unfamiliar vendors |
| Enter invoices and process payments in the accounts payable system | **Execute unauthorized payments / kickback schemes.** An employee with the ability to issue purchase orders and also process vendor invoices has too much control over the transaction. They may make personal purchases or pay inflated prices in exchange for "kickbacks" from the vendor. | **Note:** We strongly advise local governments not to give both these roles to the same person. Otherwise, consider these potential compensating controls:<br>• Review vendor payments with increased scrutiny<br>• Periodically verify goods purchased arrived on-site; monitor ship-to addresses<br>• Periodically evaluate that the vendor's efforts to carry out contracted work match expectations<br>• Evaluate pricing of goods and services for reasonableness, and monitor for significant price increases that appear unfavorable to the government |
| Prepare journal entries, or otherwise modify the general ledger | When the same employee can initiate procurements and make journal entries, they may move funds within the general ledger to conceal theft or loss of funds. | • Require secondary review of each journal entry and its supporting documentation. Be alert to journal entries directly affecting cash or reclassifications of expense.<br>• Periodically spot-check for unusual journal entries and follow up |

# Inventory

The employee tasked with looking after inventory is managing consumable supplies, goods or equipment, and ensuring they maintain the right amount in stock to meet the government's ongoing needs. Depending on your local government's role, inventory might include vehicle parts for a county vehicle repair shop, hospital supplies or pharmaceuticals, or transmission line building materials for a public utility district. The orange box in **Diagram 7** shows the position of the person directly managing inventory; this role is separate from authorizing purchases, recording the initial receipt of goods and adjusting inventory levels.

**Diagram 7** – Inventory system roles

**Table 6 –** Employee is responsible for/in charge of consumables or equipment held in inventory stores:

| Roles this employee should not have | Risk if the employee has both roles | Compensating controls to consider |
|---|---|---|
| Purchasing | **Order-and-take schemes.** Employees purchase goods that they can then use for personal purposes, privately sell, or return for credits or gift cards. | **Note:** If you have high-risk or valuable inventory, we strongly advise local governments not to give both these roles to the same person. Otherwise, consider these possible compensating controls:<br>• Perform a spot-check to ensure ordered goods arrived on-site and staff recorded it in inventory records<br>• Review inventory purchase activity for reasonableness, including nature and frequency of purchases |
| Receive and record inventory | **Skimming inventory schemes.** The employee misappropriates some or all of the stock when it arrives and then fails to record it in the inventory recordkeeping system. | Perform a spot-check to ensure ordered goods arrived on-site and staff recorded it all in inventory records |
| Adjust inventory levels | **Inventory write-off schemes.** The employee conceals their theft by adjusting inventory records, to reduce quantities on hand. | • Periodically review the inventory adjustment activity for reasonableness and trace select adjustments to support<br>• Require documentation of inventory adjustments<br>• Require secondary authorization for adjustments, or at least those exceeding a certain amount |
| Authorize inventory distributions or withdrawals | **Execute unauthorized withdrawals.** When the person responsible for maintaining inventory stocks can also authorize distribution of stock, they could more easily alter the inventory records to conceal their own improper stock withdrawals. | • Require supporting documentation for inventory withdrawals, such as a material withdrawal form<br>• Periodically compare inventory withdrawals to the underlying support and evaluate for reasonableness |

**Table 6 –** Employee is responsible for/in charge of consumables or equipment held in inventory stores:

| Roles this employee should not have | Risk if the employee has both roles | Compensating controls to consider |
|---|---|---|
| Scrapping or disposing of inventory | **Theft at disposal schemes.** When the person responsible for maintaining inventory stocks also disposes of unwanted goods, they could more easily convert them to personal use or sell them for personal gain. | **Note:** Compensating controls will vary based on the type and amount of inventory you expect to dispose of<br>• Establish clear policies concerning surplus/disposal procedures<br>• Require documentation for scrapped inventory, potentially including two-person certification for how they disposed of it<br>• Monitor inventory records and periodically trace disposals to support, including required approvals or destruction certifications<br>• Monitor the quantity and value of scrapped items or disposals to ensure it meets expectations for normal business patterns<br>• Monitor scrap revenues, if applicable |
| Conduct inventory counts or audits | When the person responsible for maintaining stock also conducts inventory counts, they could alter the inventory count results to conceal a misappropriation. | **Note:** We strongly advise local governments not to give both these roles to the same person (one should never audit themselves)<br>• Review audit documentation to ensure the employee conducted the inventory counts or audits properly<br>• Periodically conduct independent surprise inventory counts throughout the year, especially for valuable or high-risk items<br>• Review system reports for incorrect or unlikely results, such as items with negative inventory balances, and follow up |
| Prepare journal entries, or otherwise modify the general ledger | When the same employee has access to inventory and can make journal entries, they may move funds within the general ledger to conceal a misappropriation. | • Require secondary review of each journal entry and its supporting documentation. Be alert to journal entries directly affecting inventory or reclassifications of expense.<br>• Periodically review for unusual journal entries and follow up |

# Capital and other valuable assets

The employee tasked with looking after capital assets is managing durable goods that you expect them to safeguard and only use in the government's operations. Depending on your local government, capital and other valuable assets might include computers, shop equipment, heavy equipment or vehicles. The orange box in **Diagram 8** shows the position of the person managing capital and other valuable assets. This employee's role is separate from authorizing purchases, updating the asset tracking system for changes, and handling the sale or surplus of assets.

**Diagram 8** – Capital and valuable assets roles

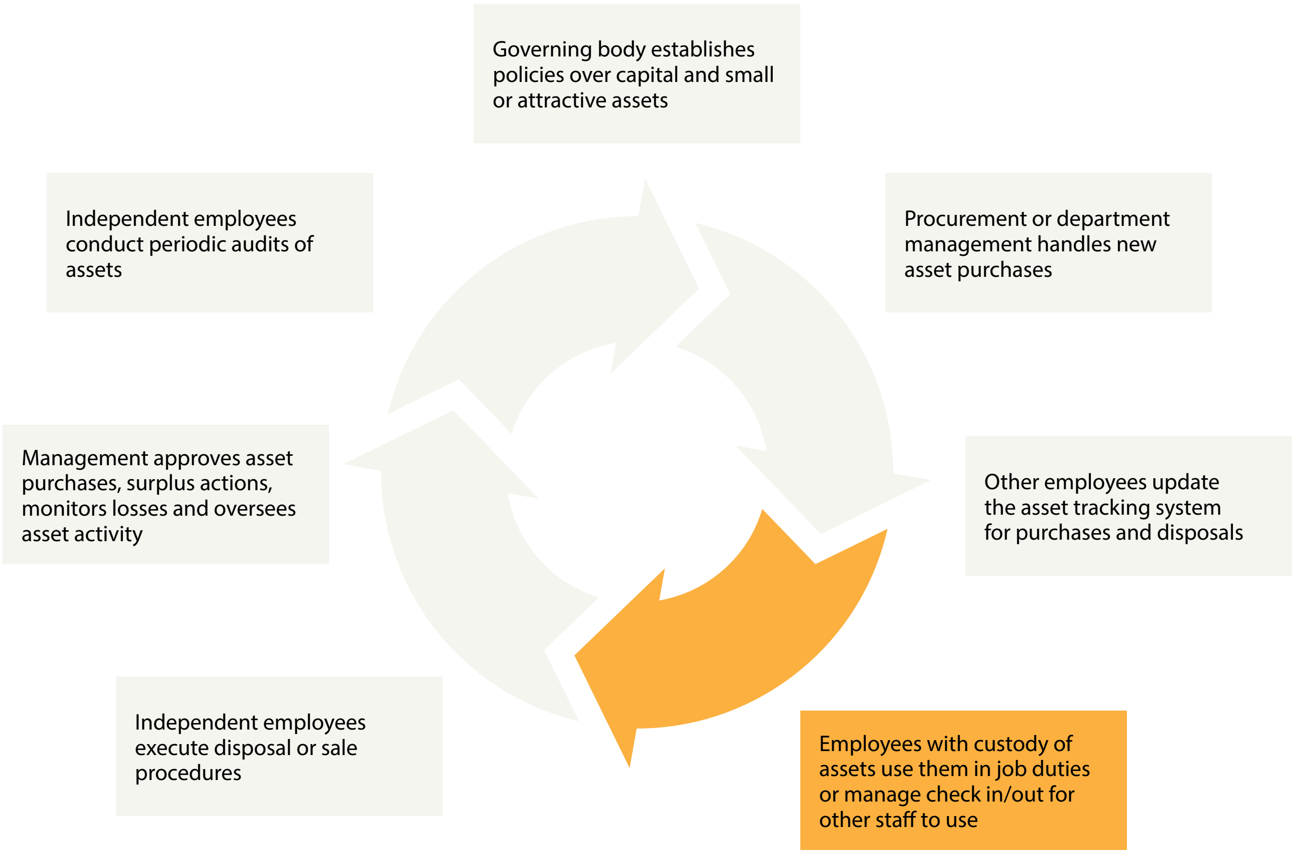


**Table 7 –** Employee is physically responsible for capital or other valuable assets (asset custodian):

| Roles this employee should not have | Risk if the employee has both roles | Compensating controls to consider |
|---|---|---|
| Authorize purchases | **Order and take schemes.** When the asset custodian can also authorize a purchase, they could order extra or unneeded equipment and convert it to personal use. | • Perform a spot-check to ensure ordered items arrived on-site<br>• Periodically review asset purchases, check that they make sense given your operational needs and replacement schedule<br>• Establish a system to track assets upon purchase and periodically conduct an internal audit of the assets tracked<br>• When approving payments, look for vendors with unfamiliar "ship-to" addresses |
| Record the asset in your asset-tracking system | When the asset custodian must also record the newly purchased asset in your asset tracking system, they may choose not to record it to conceal a misappropriation. | Periodically trace new purchases to the asset tracking system to ensure the employee recorded them |
| Modify the asset-tracking system | When the asset custodian can also modify records within an asset tracking system, they could conceal a misappropriation by deleting records. | • Only use asset-tracking software that maintains a proper audit trail, and review it for unusual activity such as deleted assets<br>• Permanently engrave all property owned by your government, upon receipt (to help deter theft)<br>• With each new asset purchase, someone independent should inquire what happened to assets that previously performed the function |

**Table 7 –** Employee is physically responsible for capital or other valuable assets (asset custodian):

| Roles this employee should not have | Risk if the employee has both roles | Compensating controls to consider |
|---|---|---|
| Conduct tasks involved in the disposing of assets, including:<br>• Authorizing disposal<br>• Making arrangements for the asset sale or disposal<br>• Physically executing the sale as the last person responsible for the item | **Theft at disposal schemes.** When the same employee has custody of assets and can arrange for their disposal, they could take the proceeds from the sale either for personal use, to spend on unallowable purposes or to convert discarded items to personal use. | • Establish clear policies concerning surplus procedures. If you allow employees to purchase surplus items, and state law does not prohibit it, ensure your policy describes the process employees must follow.<br>• Establish a secure, central file to hold titles for assets such as vehicles (and do not allow those managing assets access to them)<br>• Set up a central monitoring system, such as in finance, to ensure you receive payment for asset sales<br>• Require documentation for disposals, such as a bill of sale, record of transfer to another agency or an auction house, or destruction certification<br>• Periodically review asset disposals and the supporting documentation<br>• With each new asset purchase, inquire what happened to assets that previously performed the function |
| Conduct internal audits of capital assets | When the same employee has both custody of assets and accounts for their whereabouts, they can alter audit results to conceal a misappropriation. | **Note:** We strongly advise local governments not to give both these roles to the same person (one should never audit themselves)<br>• If it is unavoidable, at a minimum review internal audit documentation to ensure the employee conducted it properly. You should trace some select assets from the source documentation to the physical item.<br>• Periodically conduct independent surprise checks throughout the year, tracing assets from the source documentation to the physical item |

# Banking systems

One of the most important tasks in managing local government finances is to reconcile bank statements to the general ledger to ensure financial transactions occur as expected, as well as to detect any irregularities either on the bank's part or due to internal concerns. This role is shown in the orange box in **Diagram 9**. It is separate from other functions, such as those that cash receipt, process accounts payable or payroll payments, and – equally importantly – people that can sign on the government's bank accounts.

**Diagram 9** – Banking system roles

**Table 8 –** Employee reconciles the bank statement and its activity:

| Roles this employee should not have | Risk if the employee has both roles | Compensating controls to consider |
|---|---|---|
| Access to the bank deposit and the safe | **Stolen deposit.** An employee who both reconciles the bank statement and can access the bank deposit can more easily steal all or part of the deposit. | **Note:** We strongly advise local governments not to give both these roles to the same person. To uphold segregation of duties, you might consider outsourcing the bank reconciliation to a contracted accountant. Otherwise consider these possible compensating controls:<br>• Monitor deposit activity using online banking access and deposit source records (or request a mailed statement copy from the bank)<br>• Perform a secondary review of the bank reconciliation<br>• Periodically have an independent person reperform the reconciliation in its entirety<br>• Monitor revenue streams for reasonableness |
| Process payroll or accounts payable invoices (claims) | **Execute unauthorized payments.** When the same employee can both process payments and reconcile the bank statement, they might execute and conceal unauthorized payments. | **Note:** We strongly advise local governments not to give both these roles to the same person. To uphold segregation of duties, you might consider outsourcing the bank reconciliation to a contracted accountant. Otherwise consider these possible compensating controls:<br>• Monitor expenditure activity using online banking access and trace to source records (or have the bank mail you a copy of the statement)<br>• Perform a secondary review of the bank reconciliation<br>• Periodically have an independent person reperform the reconciliation in its entirety<br>• Monitor payroll or accounts payable check runs or electronic payment transactions closely, ensuring all activity is appropriate and reconciles to bank withdrawals |
| Access check payments, such as before you mail or distribute them | **Check alteration, check theft** | • Review front and back of endorsed checks for indications of alteration or theft<br>• Consider using your bank's Positive Pay service (or reverse positive pay) to detect check alterations |

**Table 8 –** Employee reconciles the bank statement and its activity:

| Roles this employee should not have | Risk if the employee has both roles | Compensating controls to consider |
|---|---|---|
| Ability to authorize payments in any form, including signing checks, approving electronic funds transfers or wire transfers or otherwise serving as a signer on the government's bank accounts | **Execute unauthorized payments.** When the same employee can authorize payments and reconcile the bank statement, they could make and conceal unauthorized payments. | **Note:** We strongly advise local governments not to give both these roles to the same person. To uphold segregation of duties, you might consider outsourcing the bank reconciliation to a contracted accountant.<br>• If it is unavoidable, at a minimum an independent person should periodically review bank account activity, using online access or by requesting a copy of the bank statement(s) directly from the bank. This independent person should perform a detailed review of expenditure activity as reflected in the banking records and trace it to support.<br>• In addition, we advise that you prohibit the clerk from sending out payments until after the governing body reviews and approves them. The governing body should play an active role and regularly ask for original support for select transactions. An independent person should monitor the banking activity for payments that bypass board approval.<br>**If you send payments electronically:**<br>• Require a second person to review the ACH payment file and authorize the bank to release funds (you can set this up with your bank)<br>• Impose a wire limit with the bank for any authorized person<br>• Require your bank to obtain secondary authorization for wire transfers, or for those that exceed a certain threshold, or that are non-repetitive<br>• Periodically compare the bank's ACH receipt to your original source records, to ensure no one diverted funds to an unauthorized bank account<br>**If you pay by check:**<br>• Use two-signature authorizations on all checks. However, some banks will not monitor this and you will need to consider other controls.<br>• Obtain endorsed, cleared checks directly from the bank and scrutinize the payments, trace to support if needed |

# General ledger

General ledger accountants prepare journal entries, record transactions or events, and make other changes to the government's general ledger. They should not have access to assets like cash, process payments or approve their own journal entries. Their role is shown in the orange box in **Diagram 10**. It is separate from other functions such as cash receipting and processing accounts payable or payroll payments.

**Diagram 10** – General ledger system roles

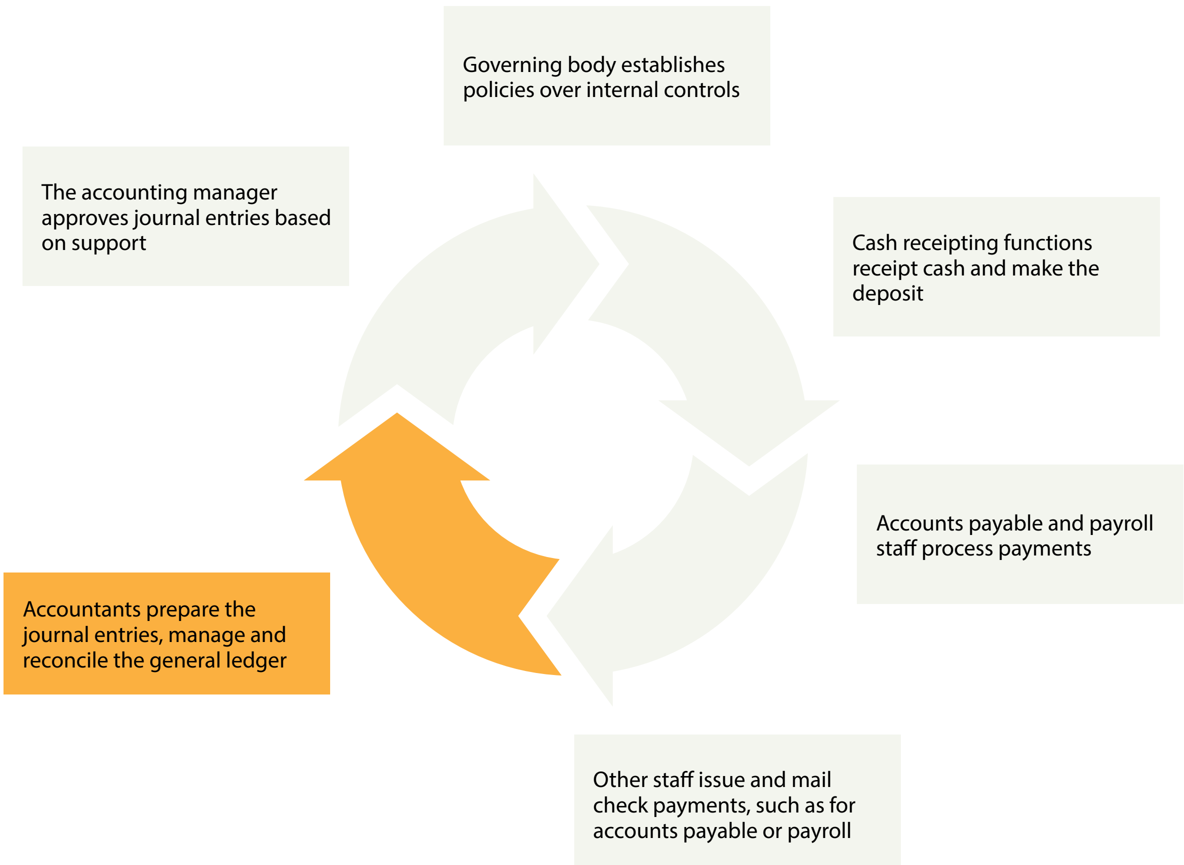


**Table 9 –** Employee performs journal entries or makes other changes to the general ledger:

| Roles this employee should not have | Risk if the employee has both roles | Compensating controls to consider |
|---|---|---|
| Access to deposits or other funds and assets | When the same employee has access to money or assets and can also make journal entries, they may move funds within the general ledger to conceal theft or loss of funds. | • Require secondary review of each journal entry and its supporting documentation. Be alert to journal entries directly affecting cash or reclassifications of revenue or expense.<br>• Periodically review for unusual journal entries and follow up |
| Process accounts payable or payroll | When the same employee can make or approve payments or payroll, and can also make journal entries, they may move funds within the general ledger to conceal theft or loss of funds. | • Require secondary review of each journal entry and its supporting documentation. Be alert to journal entries directly affecting cash or reclassifications of revenue or expense.<br>• Periodically spot-check for unusual journal entries and follow up |
| Initiate procurements | When the same employee can initiate procurements, and can also make journal entries, they may move funds within the general ledger to conceal theft or loss of funds. | • Require secondary review of each journal entry and its supporting documentation. Be alert to journal entries directly affecting cash or reclassifications of expense.<br>• Periodically spot-check for unusual journal entries and follow up |
| Approve a journal entry | When the same employee both enters and approves journal entries, fraudulent or unintentional errors that affect the general ledger can go undetected. | **Note:** We strongly advise local governments not to give both these roles to the same person. To uphold segregation of duties, you might consider outsourcing journal entry review and approval to a contracted accountant. Otherwise consider these possible compensating controls:<br>• Reconcile general ledger account balances<br>• Review the general ledger trial balance on a monthly or quarterly basis, and follow up on anything unusual<br>• Evaluate budget line item variances, as compared to actual spending, and follow up<br>• Someone independent should evaluate if the clerk completed all routine month-end or year-end adjusting entries<br>• Adopt a checklist so the clerk can double-check that they performed all routine journal entries |

# Federal awards

Those managing federal awards deal with many different compliance requirements, which can vary by award. In some cases, the traditional control system may already incorporate segregation of duties concepts. In other cases, you must design and implement special controls to address federal awards. Below are examples of segregated duties as related to the control systems for each of the common administrative requirements, as provided by the Office of Management and Budget's Compliance Supplement (Part 6, Appendix 2). In all cases, if you cannot practically segregate duties, you should select and develop alternative control activities to reduce risk of noncompliance.

To learn more about the common administrative requirements, consider referring to Section 2 of the State Auditor's Office guide: Essentials of Managing Federal Awards – A Compliance Handbook.

**Table 10 –** Segregating duties for the common administrative requirements

| Common administrative requirement | Duties to segregate | Risks of not segregating duties and if not feasible, potential compensating controls you could implement |
|---|---|---|
| Allowable costs and activities | • Initiating transactions in the general ledger<br>• Approving transactions in the general ledger<br>• Recording transactions in the general ledger | When an employee can initiate, approve and record a transaction, it gives them too much control over it. They might conceal fraud or make errors that lead to noncompliance.<br>If you cannot segregate duties, increase monitoring and oversight to ensure you reduce your risk of fraud or error.<br>For more information on segregation of duties for certain transaction types, refer to Chapters 3, 4 and 9 of this section (payroll, accounts payable and general ledger, respectively). |
| Cash management | • Processing program expenditures<br>• Processing drawdowns or reimbursement requests | The risk of not segregating these duties is that when the same person can process expenditures and claim them under a federal award, then unallowable transactions may go undetected.<br>If you cannot segregate duties, one potential compensating control is for someone knowledgeable about the federal award's requirements to periodically review drawdowns or reimbursement claims and trace information to support. |

**Table 10 –** Segregating duties for the common administrative requirements

| Common administrative requirement | Duties to segregate | Risks of not segregating duties and if not feasible, potential compensating controls you could implement |
|---|---|---|
| Eligibility | • Determining participant's eligibility<br>• Reviewing/approving participant's eligibility | The risk of not segregating these duties is that when the same person determines, reviews and approves eligibility, then they may make mistakes in applying eligibility criteria that may go undetected.<br>If you cannot segregate duties, then one potential compensating control is for someone knowledgeable about the federal award's eligibility requirements to periodically sample and verify eligibility determinations. |
| Equipment and real property management | • Accounting for property (recordkeeping)<br>• Safeguarding property (physical custody) | The risk of not segregating these duties is that an employee can conceal an asset misappropriation by failing to record a new asset, or by deleting records for an existing asset.<br>If you cannot segregate duties, then compensating controls might include:<br>• Only use asset-tracking software that maintains a proper audit trail, and review it for unusual activity such as deleted assets<br>• Periodically trace new asset purchases to the asset tracking system to ensure they were recorded<br>• Permanently engrave all property as owned by your government, upon receipt<br>• With each new asset purchase, inquire what happened to assets that previously performed the function<br>You can also find this particular risk and compensating controls described in Chapter 7 of this section. |

**Table 10 –** Segregating duties for the common administrative requirements

| Common administrative requirement | Duties to segregate | Risks of not segregating duties and if not feasible, potential compensating controls you could implement |
|---|---|---|
| Cost sharing, level of effort and earmarking | • Accounting for match, level of effort and earmarking requirements<br>• Reviewing and approving reporting of match, level of effort and earmarking requirements to the awarding agency | The risk of not segregating these duties is that when the same person performs the accounting and review/approval for these types of financial obligations, they may fail to detect their own mistakes.<br><br>If you cannot segregate duties, one potential compensating control is for someone knowledgeable about the federal award's requirements to periodically review the support and calculations. |
| Period of performance | • Initiating transactions, in the general ledger<br>• Approving transactions, in the general ledger<br>• Recording transactions, in the general ledger | When an employee can initiate, approve and record a transaction, it gives them too much control over it. They might conceal fraud that could go undetected. Or they may misinterpret or misunderstand federal award requirements and charge costs to a federal award outside the allowable timeframe (the period of performance).<br><br>If you cannot segregate duties, increase monitoring and oversight to ensure the employee understands the period of performance for each federal award, and that recorded transactions adhere to it.<br><br>For more information on segregation of duties for certain classes of transactions, refer to Chapters 3, 4 and 9 of this section (payroll, accounts payable and general ledger, respectively). |
| Procurement and Suspension and Debarment | • Initiating procurements<br>• Recording procurements in the general ledger<br>• Making disbursements | When an employee can initiate a procurement, record it and issue vendor payments, it gives them too much control over the transaction. They might conceal fraud such as one involving kickbacks or bribery, convert purchases to personal use, make errors that go undetected, or fail to comply with federal procurement requirements.<br><br>If you cannot segregate duties, increase monitoring and oversight to reduce your risk of fraud, errors or noncompliance. For more information about segregating duties for those that initiate procurements, refer to Chapter 5 of this section.<br><br>For suspension and debarment, we would expect periodic oversight to ensure staff take the steps to comply. |

**Table 10 –** Segregating duties for the common administrative requirements

| Common administrative requirement | Duties to segregate | Risks of not segregating duties and if not feasible, potential compensating controls you could implement |
|---|---|---|
| Program income | • Collecting cash or other payments<br>• Depositing cash or other payments<br>• Generating invoices (billing)<br>• Recording general ledger activity<br>• Reconciling the bank statement | The risk of not segregating these duties is that employees may misappropriate program income, as it is paid to you.<br>We cover the risks of not segregating duties and potential compensating controls for cash receipting in Chapter 1 of this section. |
| Reporting | • Preparing required reports<br>• Reviewing and filing reports | The risk of not segregating these duties is that the employee performing these conflicting tasks may report incorrectly to the awarding agency, and you will not detect it.<br>If you cannot segregate duties, one potential compensating control is for someone knowledgeable about the federal award's reporting requirements to periodically review some of the submitted reports and trace key information to underlying support. |
| Subrecipient monitoring | • Monitoring subrecipients to ensure they comply with the federal subaward<br>• Approving conclusions made about the subrecipient's compliance | The risk of not segregating these duties is that when the same person performs the monitoring and approves conclusions about subrecipient compliance, they may make mistakes that you will not detect.<br>If you cannot segregate duties, then one potential compensating control is for someone knowledgeable about the federal award's requirements to periodically review the support for the conclusions made. |

SECTION 3

# Use technology to enforce segregation of duties

You should use technology to enforce segregations of duties whenever possible. Within each software application, you typically establish each user's role and permissions. Or your system may use workflows or other automated controls to assign or restrict access. You should use these important security features to prevent users from performing tasks unrelated to their day-to-day job duties, or that you did not authorize them to perform. For example, if you allow Sally to approve timesheets, but not Scott and Alice, you should restrict Scott and Alice from approving timesheets within your software application. Then, the application will block them and effectively enforce segregation of duties.

To do this effectively, follow these best practices:

## Setting yourself up for success

- Develop and implement policies and procedures to guide employees using your software application's security features to manage or restrict access.
- When you assess potential software purchases, consider the security features that will allow you to enforce segregation of duties.
- Use your IT department to manage the security features within software applications that allow you to enforce segregation of duties. If IT staff require training, then provide it.

  Department managers often want to control software application access because they understand all staff assignments, but it usually creates too much risk. The reason this practice is risky is that then the department manager has unfettered access to all system functions, or they can give themselves unfettered access, and perpetrate fraud – likely without detection as there is no one to monitor their activities.

  If you lack the IT staff, then assign someone with little to no responsibilities associated with the application or its related processes.

## Restricting access

- Only grant each user the access that they need to perform their day-to-day job and nothing more. You should not give ongoing access for temporary needs, occasional duties or future possibilities.

- Make sure that no single user has the ability to perform multiple parts of the same transaction flow – this gives them too much control. Specifically, make sure that no single user can initiate, process, post, adjust and approve a transaction.
- Grant read-only access when users need to see information, but do not need to edit.
- Limit administrative or superuser access to software applications as much as possible, even within the IT department.

## Managing access under special circumstances

- Employees occasionally cover other employee duties, such as during a leave of absence. Grant temporary additional system access only for the timeframe employees need them.
- Remove access promptly when the user no longer needs it, such as when the user's job duties change, they transfer to another department or they separate from the government's employment.
- If you allow employees additional access during a software implementation, make sure to refine and restrict them as soon as you can.

## Monitoring access

- Regularly review system access at least annually. If you have staffing changes or system updates, you may want to review it more frequently.
- If you implement a new system, review system access more frequently in the implementation year. You will learn more about how the system works, gain comfort in using it, and can work to refine the security features that restrict or manage access.

If you cannot enforce segregation of duties using software security features, then you should implement compensating controls to reduce risk to an appropriate level. See Section 2 of this guide.

APPENDIX A

# Example of duty assignments for small governments

## One-person accounting department

When you give one person many duties and responsibilities, several risks arise. To adequately mitigate risk, you will need at least one other person to provide oversight. Among your options:

- One or more members of the governing body
- An outside contractor, such as a local accounting firm
- A task exchange with a nearby government, in which you perform oversight functions for each other

Whichever solution you choose, make sure the person involved understands the risks that can arise when you do not segregate duties. (A review of the Risks column in Section 2 can help.) **Table 11** illustrates one way a local government might organize duties in a one-person accounting department.

**Table 11:** One way to organize a one-person accounting department

| Duty | Clerk | Oversight person |
|---|---|---|
| Cash receipt | Collect receipts from customers, prepare the deposit and make the deposit with the bank | **No access to money or the deposit.**<br>• Monitor to ensure the employee made the entire deposit by comparing validated bank receipts to source records. This should include confirming that cash vs. check composition is correct.<br>• Monitor the daily deposit for reasonableness, including the amount of cash<br>• Monitor voided receipts<br>• Authorize any customer refunds<br>• Might do a last look at the deposit periodically to ensure you only observe customer checks (in the presence of the clerk who prepared the deposit/do not take sole custody of it) |
| Accounts receivable | Send out billings, post payments to accounts and perform collections | • Monitor monthly revenue reports and adjustment activity to customer accounts<br>• Monitor collection efforts, review the accounts receivable aging report<br>• Approve customer account adjustments or write-offs |

**Table 11:** One way to organize a one-person accounting department

| Duty | Clerk | Oversight person |
|---|---|---|
| Payroll | Process and prepare checks (or use a third-party vendor or county auditor if possible) | Approve time sheets, approve pay increases, review and approve the payroll register, and sign and distribute checks |
| Accounts payable | Process invoices (claims) and prepare checks (or use county auditor) | Review supporting documentation, approve invoices (claims) acting as the auditing officer, sign and mail checks |
| Purchasing and procurement | Obtain or review quotes or bids | Review quote or bid results, and sign all contracts or purchase orders |
| Capital assets | Maintain a listing | Periodically conduct a physical inventory |
| Banking | Prepare the bank reconciliation | • Act as the signer on the account<br>• Monitor banking activity using online account or by having the bank mail the original statement directly to you, along with the copies of endorsed checks<br>• Review the bank reconciliation |
| General ledger | Perform journal entries | Review and approve journal entries |

## Two-person accounting department

A two-person department allows for some separation of duties, especially if they can rotate duties periodically to further strengthen controls. But conflicting duties are still present. To adequately mitigate risk, you will need at least one other person to provide oversight. Among your options:

- One or more members of the governing body
- An outside contractor, such as a local accounting firm
- A task-exchange with a nearby government, in which you perform oversight functions for each other

Whichever solution you choose, make sure the person involved understands the risks that can arise when you do not segregate duties. (A review of the Risks column in Section 2 can help.) **Table 12** illustrates one way a local government could organize duties in a two-person accounting department.

**Table 12:** One way to organize a two-person accounting department

| Duty | Clerk 1 | Clerk 2 | Oversight person |
|---|---|---|---|
| Cash receipt | Perform receipting, prepare the deposit and deliver the deposit to the bank (if needed)<br>Clerk 1 and Clerk 2 open mailed payments together and log them | Backup cash receipt, but limit access as much as possible to all receipts and the deposit<br>Clerk 1 and Clerk 2 open mailed payments together and log them | **No access to money or the deposit.**<br>• Compare validated bank receipts to source records to ensure the employees made the entire deposit. This should include confirming that cash versus check composition is correct.<br>• Monitor the daily deposit for reasonableness, including the amount of cash<br>• Monitor voided receipts<br>• Authorize any customer refunds<br>• Might do a last look at the deposit periodically to ensure you only observe customer checks (in the presence of the clerk who prepared the deposit/DO NOT take sole custody of it) |
| Accounts receivable | No duties | Send out billings and manage customer accounts, collections and concerns | • Monitor monthly revenue reports and adjustment activity to customer accounts<br>• Monitor collection efforts, review the accounts receivable aging report<br>• Approve customer account adjustments or write-offs |
| Payroll | Edit the payroll master file, review the preliminary payroll register and prepare checks or initiate the direct deposit ACH file | Process the payroll, tax filings | • Approve timesheets and pay rates/ pay increases<br>• Review the final payroll register and authorize payroll payments, including signing checks<br>• If you use direct deposit, act as approver for the bank to release the ACH payments (you must set this up with your bank) |

**Table 12:** One way to organize a two-person accounting department

| Duty | Clerk 1 | Clerk 2 | Oversight person |
|---|---|---|---|
| Accounts payable | Process invoices (claims), prepare checks | Edit vendor master file | Review supporting documentation, approve invoices (claims) acting as the auditing officer, sign and mail checks |
| Purchasing and procurement | Be present for sealed bids openings, for contracts of a certain size | Obtain and review bids | Review bid results and approve purchases, approve contracts |
| Capital assets | Maintain a listing | Periodically conduct a physical inventory | Review the inventory results and asset listing |
| Banking | None (too many conflicting duties to have this task) | Reconcile the bank activity | • Act as the signer on the bank account<br>• Monitor banking activity using online account or by having the bank mail the original statement directly to you with copies of endorsed checks. Check that expenditure activity has been authorized and is appropriate<br>• Review the bank reconciliation |
| General ledger | Prepare journal entries | Review and approve journal entries | Optional review |

## Three-person accounting department

You can more readily distribute accounting duties between three employees, than occurred with the one- and two-person accounting departments. However, you still need to practice oversight, but that oversight person has less risk to worry about so their job becomes easier. **Table 13** illustrates one way a local government might organize duties with a three-person accounting department.

**Table 13:** One way to organize a three-person accounting department

| Duty | Clerk 1 | Clerk 2 | Clerk 3 | Oversight person |
|---|---|---|---|---|
| Cash receipt | Receipt cash from customers and take the deposit to the bank.<br>Clerk 1 and Clerk 2 open mailed payments together and log them. | • Backup cash receipt<br>• Prepare the deposit<br>Clerk 1 and Clerk 2 open mailed payments together and log them. | **No access to money or the deposit.**<br>• Monitor to ensure Clerk 1 made the deposit intact by comparing the validated bank receipt to source records. This should include confirming that cash versus check composition is correct.<br>• Monitor void receipts. | **No access to money or the deposit**<br>• Authorize any customer refunds<br>• Monitor the daily deposit for reasonableness, including the cash amount<br>• Might do a last look at the deposit periodically to ensure you only observe customer checks (in the presence of the clerk who prepared the deposit/DO NOT take sole custody of it). |
| Accounts receivable | No duties | No duties | Post payments to customer accounts, send out billings, handle collections, execute any account adjustments | • Approve customer account adjustments or write-offs<br>• Monitor collection efforts, review the accounts receivable aging report |

**Figure 3:** One way to organize a three-person accounting department

| Duty | Clerk 1 | Clerk 2 | Clerk 3 | Oversight person |
|---|---|---|---|---|
| Payroll | Prepare the payroll checks or initiate ACH direct deposit with the bank. | Process time sheets and payroll, create preliminary payroll register | **No access to process payments**<br>• Serve as the auditing officer.<br>• Add new employees and wage rates/edit payroll master file.<br>• Review the preliminary and final payroll register and monitor the completion of payroll tax filings. | • Approve time sheets, pay increases, pay rates<br>• Authorize payroll payments including signing checks and giving approval of the ACH file (you do this directly with the bank, so that it will release the payments) |
| Accounts payable | Process invoices (claims) for payment | Prepare the accounts payable checks or initiate ACH direct deposit with the bank. | **No access to process payments**<br>• Edit vendor master file – add new vendors<br>• Serve as auditing officer – audit accounts payable claims before payment issues | • Sign checks<br>• If you send payments electronically, give approval for the bank to release the ACH file |
| Purchasing and procurement | No duties | Obtain and review bids | Be present for sealed bids openings | Authorize purchases, procurements and contracts |
| Capital assets | Maintain a listing | Option to review the listing and inventory | Conduct a physical inventory | No duties |
| Banking | No duties | No duties | Reconcile the bank activity | • Act as the signer on the account.<br>• Review the bank statement and the reconciliation in detail and consider using online banking to monitor activity. |
| General ledger | | | Prepare journal entries | Review and approve journal entries |

APPENDIX B

# Self-assessment checklist

Using this checklist, you can quickly evaluate whether your government has segregated duties. You can evaluate each financial process or select just one to focus on. You can also use it to assess whether compensating controls sufficiently reduce risk to an acceptable level, in those areas where you cannot feasibly segregate duties. We publish this document separately, in an excel format. You can find it in our Resource Library.

Center for Government Innovation

## Segregation of Duties Self-assessment Checklist

| | |
|---|---|
| **Date of review:** | |
| **Completed by:** | |
| **Key recommendations:** | |

**Instructions:** Use this checklist to find areas where you do not segregate duties. You can either fix the issue by separating those duties, which is ideal (read the cell comment if you want to know why), or review your compensating controls to see if they lower your risk to an acceptable level. You may need more than one compensating control to lower your risk to a reasonable level.

| | | | Complete this section if you plan to rely on compensating controls | | | |
|---|---|---|---|---|---|---|
| | | **Answer** | **Define your risk tolerance** | **Describe compensating control(s) you have in place that address the risks created by lack of segregation of duties** | **Are these controls sufficient to lower your risk?** | **If you answered no, in the prior column, describe what additional controls you will put in place** |
| *Examples* | | | | | | |
| | *Do any cashiers issue receipts without direct supervision?* | *Yes* | *Low* | *We have a sign telling customers to expect a receipt at the park entrance* | *No* | *We will add a requirement that the customer place the receipt on their vehicle dash and we will tow vehicles without it* |
| | *Can any cashier, or anyone with access to the customer payments or the deposit, void receipts or issue refunds to customers?* | *No* | | | | |
| **Section 1. Conflicting duties for a cashier, or anyone with access to customer payments** | | | | | | |
| 1.01 | Do any cashiers accept customer payments and issue receipts without direct supervision? | | | | | |
| 1.02 | Can any cashier, or anyone with access to the customer payments, also void receipts or issue refunds to customers? | | | | | |
| 1.03 | If applicable, do any cashiers accept payments and also admit entry (such as into an event)? | | | | | |
| 1.04 | Do any cashiers, or anyone with access to customer payments, also open mail payments? | | | | | |
| 1.05 | If cashiers accept payment for goods, can any of them also perform inventory adjustments? | | | | | |
| 1.06 | Can any cashier, or anyone with access to customer payments, also generate or modify customer billings? | | | | | |
| 1.07 | Can any cashier, or anyone with access to customer payments, also adjust customer account balances? | | | | | |

# My notes

# More information

## The mission of the Office of the Washington State Auditor

To promote accountability and transparency in government.

The results of our work are widely distributed through a variety of reports on our website. We take our role as partners in accountability seriously. We provide training and technical assistance to governments and have an extensive quality assurance program.

For more information about the State Auditor's Office, visit www.sao.wa.gov.

## Americans with Disabilities

In accordance with the Americans with Disabilities Act, this document will be made available in alternative formats. Please email Communications@sao.wa.gov for more information.

## State Auditor's Office contacts

**State Auditor Pat McCarthy**
564-999-0801, Pat.McCarthy@sao.wa.gov

**Kelly Collins – Deputy State Auditor**
564-999-0807, Kelly.Collins@sao.wa.gov

**Scott Woelfle – Director of Quality Assurance and Innovation**
509-870-6946, WoelfleS@sao.wa.gov

**Debbie Pennick – Assistant Director for the Center for Government Innovation**
564-999-0818, PennickD@sao.wa.gov

**Niles Kostick – Center Program Manager**
564-999-0816, KostickN@sao.wa.gov

**Kathleen Cooper – Director of Communications**
564-999-0800, Kathleen.Cooper@sao.wa.gov

## To request public records

**Public Records Officer**
360-725-5617, PublicRecords@sao.wa.gov

"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

**1-564-999-0818**

Office of the Washington State Auditor