Segregation of Duties

Essential Internal Controls

Why it matters
How to get started
Helpful hints for small governments
Plus, self-assessments and checklists

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

First edition, September 2019

Six Golden Rules to Help Protect Your Government's Assets

1. **Separate conflicting duties whenever it is feasible with your current staffing levels.**

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

3. **Document the controls you put in place and include them in policy, so expectations are clear to employees and management alike.**

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

5. **Align user access and permissions in your financial software with the job responsibilities of each user: no more, no less, access than they need to do their jobs.**

6. **Review and reevaluate the internal controls you've put in place regularly, especially during times of change. For example: when new software is installed, when staff leave or are hired, or when job duties have changed.**

Table of Contents

Disclaimer

This guidance is intended to supplement information management should consider when establishing internal controls. The guidance might not include all information that should be considered and is not intended to supersede management's judgement in establishing internal controls, including regularly monitoring risks and ensuring internal controls are in place to address potential areas of concern.

Section 1 – Separating conflicting duty assignments can help protect your local government's assets

Every government in Washington, no matter how wide-ranging 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 fewer than 20 or even 10 employees – struggle to live up to its expectations. 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 hands take in a customer's cash payment, write out the deposit ticket, walk it to the bank, and balance the 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 join them.

We assume that 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.

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 detect errors or fraudulent activity. It is a best practice for all local governments to follow as best they can with current staffing. This guide, issued by the Center for Government Innovation, offers even the smallest governments guidance so they can put in place compensating controls that can help mitigate 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 should be 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
- Identifying particular risks associated with specific incompatible duty assignments
- Control options to help minimize the risk when you can't separate tasks
- Using features in financial software to align job responsibility with user access and permissions
- Strategies to help assign tasks and responsibilities to separate elements of closely related tasks in a small office with one, two or three employees

First, some basic concepts

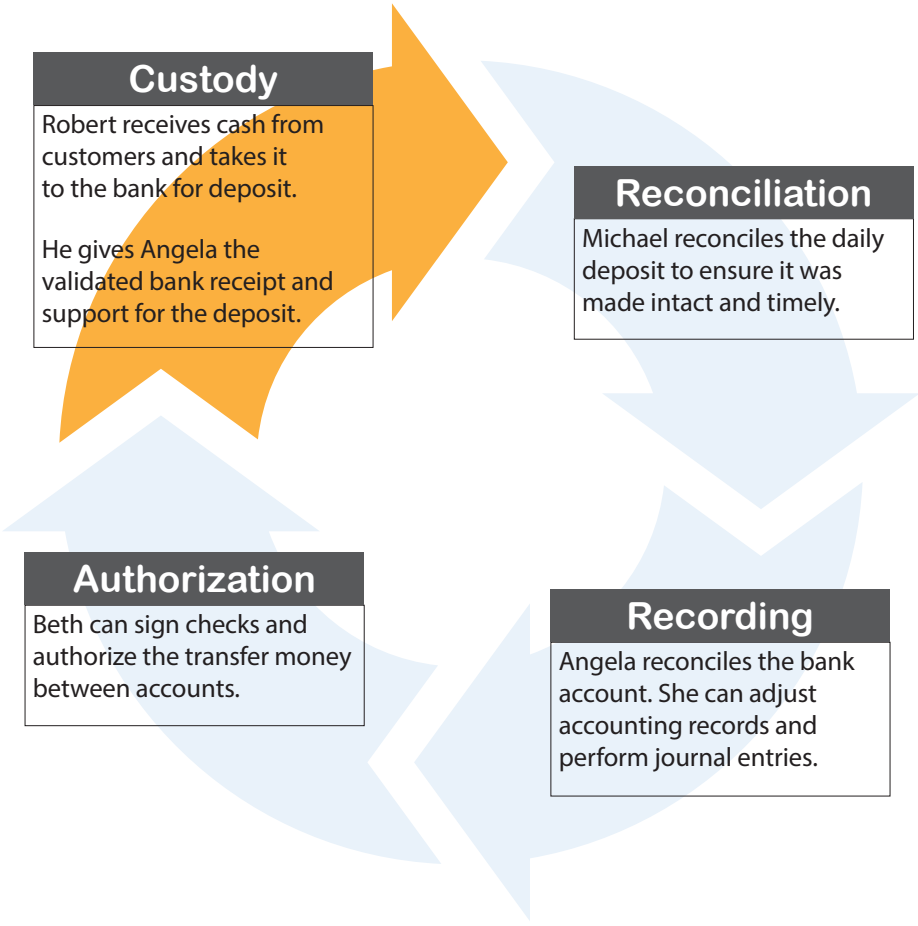
Separating duties involves assigning responsibilities to employees in a manner that reduces risk of fraud or error occurring or going undetected. When incompatible over-lapping duties are unavoidable, you must rely on controls that compensate for the risks and that include adequate monitoring and managerial oversight. Well-designed controls not only help prevent fraud or theft, but also make it easier to catch mistakes and to hold staff accountable should loss or errors occur.

Because there are many ways to attain effective internal control, the specific controls in place may look very different from one government to another. The State Auditor doesn't require any specific controls, but when we audit your government, we consider whether the procedures you've put in place provide reasonable assurance that they meet compliance and financial reporting objectives. And because you are ultimately responsible for both achieving your government's objectives and deciding the design and operation of controls, the burden of showing they are adequate rests with you.

An example of well-separated responsibilities

Banking responsibilities are a perfect example of tasks that should be performed by different people. This illustration shows how the roles of holding cash (Custody), adjusting accounting records (Recording), ensuring the deposit has been made correctly (Reconciliation), and transferring funds (Authorization) have each been held at arm's length.

As you see, Robert may handle cash, but he can't adjust entries in the general ledger or accounting records, or move funds between accounts. Michael, Angela and Beth do not have access to customer payments. Separating duties like this helps reduce the risk of theft because no one employee has too much control over a process. This local government has minimized opportunities for someone to commit fraud or make significant errors in this particular receipting process without it being detected. Identifying which duties are conflicting can be challenging, but typically they follow the custody, recording, reconciliation and authorization framework shown here.



Within the office, an employee who has no access to cash or related deposits can be considered "independent" when reconciling the deposits between bank records and system reports. An independent reviewer can identify and report discrepancies, such as a missing deposit, without being implicated in the misappropriation. But for some small governments, designing a cash receipting system like the one in our example might be close to impossible if limited staffing means there's only one employee to perform all these roles.

The independent reviewer gains importance when you cannot separate duties among different employees. The compensating controls you put in place will typically call for additional monitoring and oversight, which means the reviewer must understand the risks being monitored if you are to successfully prevent errors, fraud or theft. For independent oversight, 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 accountant to provide periodic reviews.

The next few pages list some overarching changes you can make to your organization's expectations, policies and procedures. The chapters in **Section 2** address in more detail the risks posed when your employees are carrying out conflicting assignments, with compensating controls you might put in place to reduce the risks. **Section 3** considers the risks posed by your financial and accounting software. **Appendix A** sets out some strategies for small offices with one, two or three employees. Finally, **Appendix B** has a detailed checklist to help you assess where your government stands.

Just 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 worthwhile effect. Here are some ideas that can deliver a far-reaching effect on the control structures of your local government. Some need only minimal resources to put in place.

1. Begin by reflecting on the tone you want to set from the top of your organization, as elected officials, executives and department managers. The standards you want to guide your employees' behavior – and of course, your own – can then become policies. Policies should incorporate actions and procedures, and where necessary, detail the consequences of 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 audit recommendations are followed up on.

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 with staff if actual results are not in line with expectations.

Observant Get to know your employees. Pay attention to changes in lifestyle or financial pressures. Watch for red flags in behavior, such as working late or on weekends, or resisting 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 what your expectations are concerning accountability and ethical behavior. It should be clear you will hold staff accountable and monitor activities.

2. Having established the standards you want to see followed and embraced, formalize them in policies that all employees are expected to understand and agree to. Policies around financial and accountability practices might include:

Ethical behavior. Items to consider include reporting and addressing conflicts of interest. Include expectations of employees in policy, whether that be a cash receipting, travel, or any other policy addressing how employees should carry out financial transactions when conducting government business

Establish a whistleblower policy or other mechanism so that employees can share concerns in a safe setting.

Background checks. Establish which positions are subject to mandatory background checks and/or bonding.

Vacation leave. Set and enforce mandatory annual leave for fiscal staff at all levels. Establish how and when people are authorized to step in to perform a colleague's tasks during vacation or sick leave. Make it clear work will not be held while anyone is away.

Performing a risk assessment. Establish how and when the leadership team should conduct a robust internal risk assessment process that considers internal control systems, fraud risks, along with other enterprise risks. The assessment should include an evaluation of software system weaknesses that might increase risk for fraud or errors.

Managing financial and enterprise software. As part of software management, consider who controls installation and updates, and the corresponding user permissions. Establish the policy and procedures to be used to reevaluate software access, especially during periods of change (such as software implementations, staff turnover, new or eliminated positions) when duties might evolve or shift over time, and how to de-authorize a staff member's access to a portion of the system when no longer needed.

3. Policies are most effective when followed through with practices and actions. Among the many elements that might arise as you plan and write policies, these are particularly relevant to reducing financial risk.

Training.

- Make sure employees understand 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.

- 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, and follow up on any you discover.
- Periodically conduct unannounced spot checks, for example of bank deposits.

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

- Accounts payable processed by the county auditor
- Payroll managed by a contracted payroll service
- Bank account reconciliation performed by a contracted accountant
- Independent oversight or services performed as a trade with another government

Section 2 – 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. A diagram shows that role's relationship to others whose duties should be segregated from its own. The key role is highlighted. Finally, a table with three columns sets out related but conflicting responsibilities the employee might be assigned.

- 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 actions you can take to reduce the related risk.

Ideally, your local government looks just like the diagram on page 5, with enough staff to eliminate conflicting job duties. But we recognize this is often impractical or impossible. Even large, generally well-staffed governments can have conflicts between duties, for example in a small department like cash receipting, or when an employee is out sick or on vacation and someone else must cover their work. That's where the suggested compensating controls in the third column come into action. It might take a combination of several controls, carefully chosen using your best judgment or the advice of an accounting professional, to effectively reduce risk.

Even if they can't eliminate the risk of the conflicting duty entirely, when used effectively, these controls can help reduce risk to an acceptable level.

1. 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 1**. It is separate from other functions such as roles that prepare customer billings, post payments to customer accounts, or perform oversight of the deposit (reconciliation controls).

Diagram 1 – Cash receipting roles

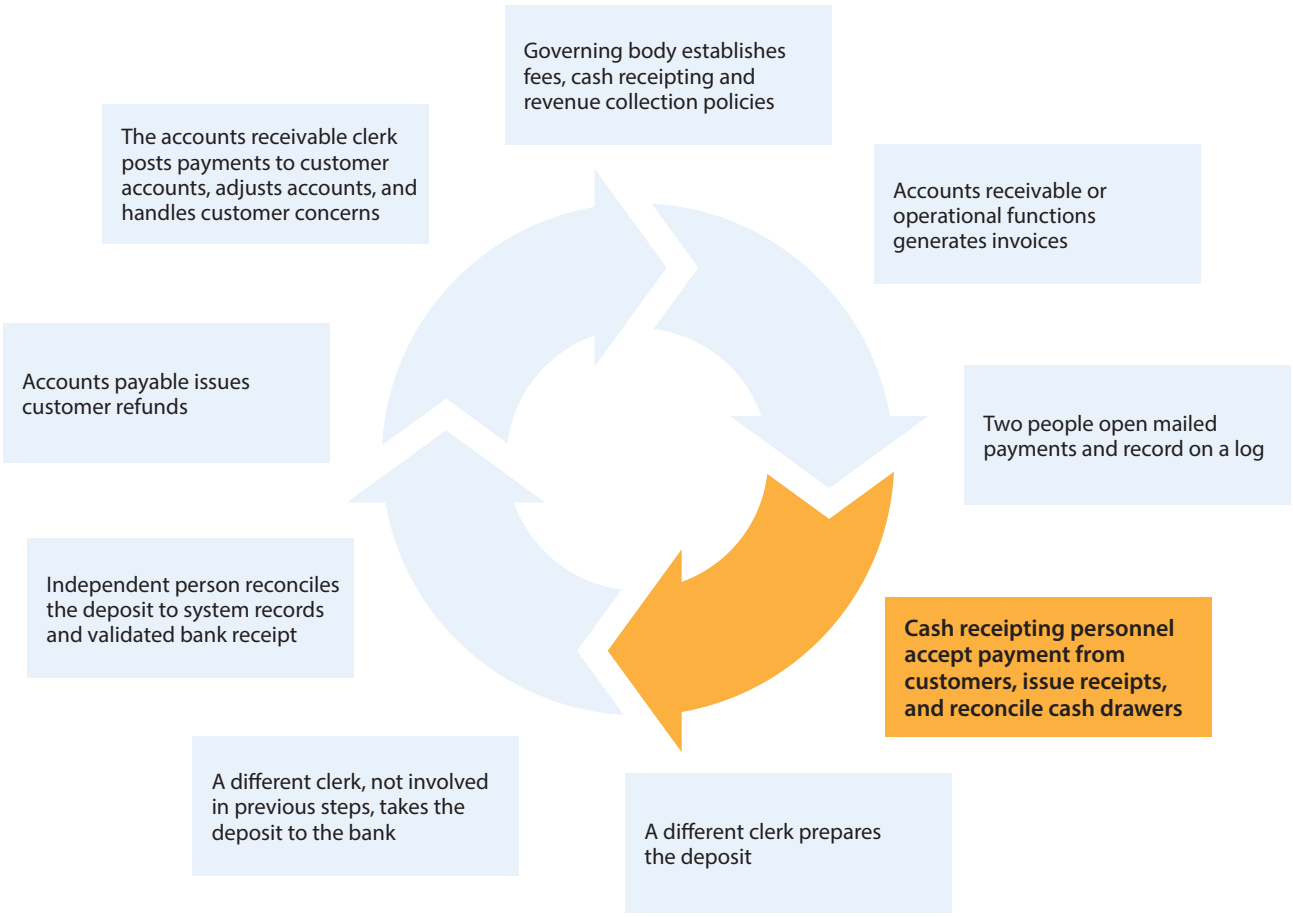


Table 1 – If the employee's job is to receive payments and produce receipts for customers, or have other access to money, whether cash or checks, for deposit, then:

Other roles this employee should not have	The risk if the employee does both roles	The compensating controls you could put in place include
Issuing receipts without supervision	**Skimming schemes.** One version involves taking cash before it has been recorded or before issuing a receipt for the payment. Another trick involves using a manual or unauthorized receipt book, to hide the funds that are pocketed. **Note**: Risk for such schemes is lower when all cash intake is expected. However, even in these settings, unexpected or miscellaneous revenues can be at risk.	• Place surveillance cameras on receipting operations • Place signs telling customers to expect a receipt, and urging them to contact a manager if they have concerns • Use cash drawers that capture zero receipts (drawer was opened but no receipt was given) • Monitor the daily deposit for reasonableness, in total and amount of cash • Conduct surprise cash counts, and look for unauthorized receipt books during the count • Put in place additional controls to monitor unexpected revenue streams • Conduct an internal audit test: Have an auditor pose as a customer, pay in cash, and not ask for a receipt. Assess whether the funds are properly recorded and the cashier insisted on providing a receipt. • Monitor inventory for unexplained shortages
Void receipts or issue refunds	**Reversing transaction schemes.** Deposits can be misappropriated and concealed by voiding a receipt or issuing a 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. • Excessive voided sales, as noted in voided transaction report, should be investigated • Require management approval for voids or refunds above a certain dollar amount
Accept cash and admit entry (such as into an event)	**Skimming scheme.** Without a ticket taker to confirm payment was made, it is easier for the person taking payments to skim some of the cash received.	• Whenever possible, do not hold ticketless events • Post a sign telling customers to expect a receipt or numbered ticket, and to tell a manager if they don't get one. • Check revenue generated meets expectations • Perform surprise cash counts

Table 1 – If the employee's job is to receive payments and produce receipts for customers, or have other access to money, whether cash or checks, for deposit, then:

Other roles this employee should not have	The risk if the employee does both roles	The compensating controls you could put in place include
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 was collected and recorded earlier. **Stolen checks**	• Require the employee to open mail in a supervised area, and as soon as all mail has been opened, endorse checks with the government's banking information and prepare the deposit. • Place surveillance cameras where mail is opened • Put in place additional controls to monitor infrequent and unexpected revenue streams • Contract out payment processing to a third party that has the desired controls • Periodically compare bank-validated deposit receipts to cash-receipting system reports to confirm the deposit's cash/check composition agrees with what has been received and recorded in the system.
Bill for goods or services	A clerk who can modify the customer's invoice so that it demands more than is actually due, and also then open the over-payment when it arrives, is in a position to skim the amount over-paid.	• Periodically trace transactions through the accounting system from origination to billing to payment as a spot check, possibly during an internal audit. • Periodically review billings before they are mailed • Independently send customers a separate statement, asking them to call management directly with questions about their bills. • Monitor active accounts to ensure all are being correctly billed for services. For example, many utilities can produce account reports to identify any with high or low billings.
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 • Periodically review customer account adjustments for reasonableness and for the presence of supporting documentation • Independently send customers detailed statements reflecting all activity on their account. Ask them to call management directly with questions about their bills.
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 were sold without a record of the sale.	• Require documentation for inventory adjustments, including management approval • Periodically review inventory adjustments for reasonableness and the presence of supporting documentation

Table 1 – If the employee's job is to receive payments and produce receipts for customers, or have other access to money, whether cash or checks, for deposit, then:

Other roles this employee should not have	The risk if the employee does both roles	The compensating controls you could put in place include
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. **Over-posting schemes.** When the cashier can also mark accounts as paid, it is easier to conceal stolen deposits by recording more payments than were received.	**Particularly for lapping schemes:** • Periodically spot-check how payments have been applied to accounts, and compare date of payments with the date of posting on the accounts. • Monitor employees regularly working late hours or not taking vacations • Monitor accounts receivable aging reports for changes from past history • Monitor and enforce a collection policy • Independently send customers detailed statements reflecting all the activity on their account. Ask them to call management directly with questions about their bills. **Particularly for over-posting schemes:** • Reconcile and monitor that the funds deposited agree with the payments posted to customer accounts **Addresses both risks:** • Require daily balancing to cash-receipting system reports for all deposits
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.	• Another employee or manager reviews a deposit before it goes to the bank to ensure cash/check composition agrees with what is recorded in the cash-receipting system. • Ask the bank to periodically return the deposit for review and analysis by management • Conduct a surprise cash count to look for personal checks in the deposit

Table 1 – If the employee's job is to receive payments and produce receipts for customers, or have other access to money, whether cash or checks, for deposit, then:

Other roles this employee should not have	The risk if the employee does both roles	The compensating controls you could put in place include
Taking the deposit to the bank	**Shorting or missing deposit.** A clerk who both accepts money and takes the deposit to the bank can more easily steal part or all of the deposit. **Delayed deposits.** When the deposit isn't made promptly, the delay increases opportunities for tampering or theft. This includes check-for-cash substitutions and borrowing schemes.	• Independently reconcile the deposit to ensure it was intact and timely • Establish a policy that sets out the frequency of deposits. State law (RCW 43.09.240) calls for deposit within 24 consecutive hours of receiving the money. If this is not practical for your government, you can apply for a waiver from the county treasurer's office, but you must comply with the 24-hour rule until you receive it. • Monitor to ensure the deposit is done daily or as expected • Ask the bank for a validated receipt with cash and check components to help monitoring efforts
Reconcile source records for the deposit to 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. • If it is unavoidable, at a minimum an independent person should periodically review the reconciliation to ensure deposits are made intact and on time.
Reconcile the general ledger to bank statements	**Stolen deposit**, in part or in full	• **Note:** We strongly advise local governments not to give both these roles to the same person. • If it is unavoidable, at a minimum an independent person should periodically review the bank reconciliation to ensure all money collected is accounted for in the general ledger. • Periodically have an independent person perform the reconciliation in its entirety
Participate in accounts payable functions	A clerk who can both receive cash and issue checks can issue checks to backfill shorted deposits into the bank account. In other words, cash could be withdrawn from the deposit and the government's own check substituted for stolen cash.	• Thoroughly review accounts payable payments • Periodically review the composition of a deposit right before it is taken to the bank. For example, look for checks other than those from customers. • Check the deposit records to ensure cash/check composition agrees with what is recorded in the cash-receipting system.

2. Accounts receivable

Accounts receivable oversees customer accounts and activity, posting payments, and performing 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 2**. It is separate from other functions such as roles that receipt cash, generate billings or process customer refunds

Diagram 2 – Accounts receivable roles

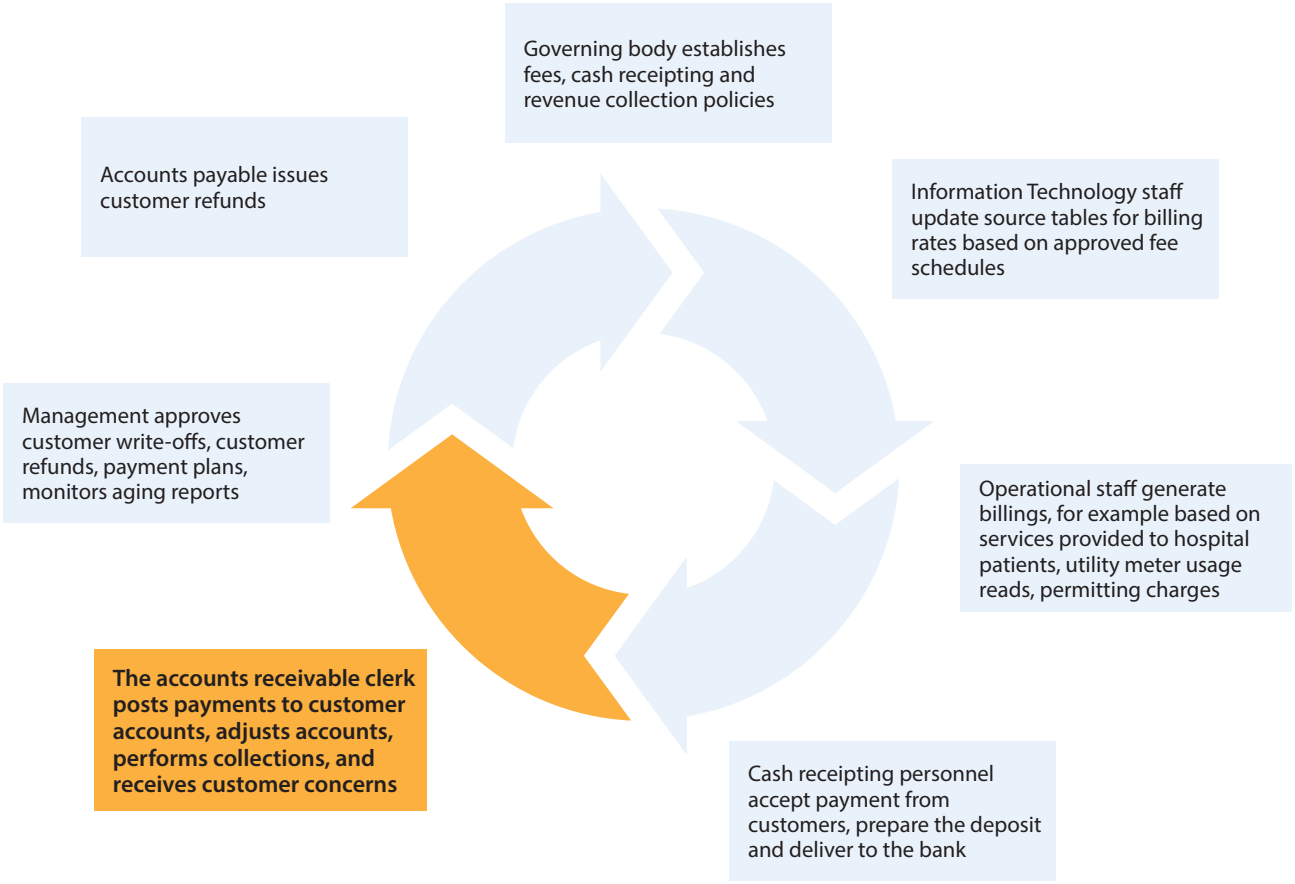


Table 2 – If the employee's job is to handle customer accounts and collections as accounts receivable, then:

Other roles this employee should not have	The risk if the employee does both roles	The compensating controls you could put in place include
Have or take custody of cash or checks, including: • Acting as a primary or backup cashier • Handling or having access to deposits • Access to mailed payments, including non-routine 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. **Write off schemes**. When the accounts receivable clerk also takes in cash or checks, it becomes easier to conceal a theft by adjusting the customer's account to reduce the amount owed and pocketing the balance. **Over-posting schemes.** When the cashier can also mark accounts as paid, it is easier to conceal stolen deposits by recording more payments than were received. **Other risks** might be present depending upon extent and nature of cash receipting duties. See the Chapter 1, Cash Receipting, for more information.	**Particularly for lapping schemes:** • Periodically spot check how payments are applied to accounts • Monitor employees regularly working late hours or not taking vacations • Require daily balancing of all deposits, including mode of payment, to cash-receipting system reports • Develop and enforce a collection policy that includes monitoring all collection efforts. • Monitor accounts receivable aging reports for changes from past history **Particularly for write-off schemes:** • Require supporting documentation for all customer account adjustments • Periodically review account adjustments **Addresses lapping and write-off:** • Independently send customers detailed statements reflecting all activity on their account. Ask them to call management directly with questions about their bills. **Particularly for over-posting schemes:** • Reconcile and monitor that the funds deposited agree with the payments posted to customer accounts
Be responsible for managing the billing/ invoicing system, including updating it for billing rates and editing billings, and sending out invoices	When the clerk responsible for cash receipting also bills customers, it is easier to manipulate invoices to collect more than is expected, steal the excess, and conceal the theft. If the accounts receivable clerk does not have access to deposits, then the risk is limited to having too much control over the process, and that errors may occur which go undetected. Note: Only a few employees should have access to the billing source tables to reduce the risk of errors and accidental changes.	• Periodically trace transactions through the billing system from origination to billing to payment as a spot check • Periodically review invoices before they are mailed • Independently send customers detailed statements reflecting all activity on their account. Ask them to call management directly with questions about their bills. • Monitor active accounts to ensure all are being correctly billed for services. For example, many utilities have reports for accounts with missing meter reads and high or low billings.

Table 2 – If the employee's job is to handle customer accounts and collections as accounts receivable, then:

Other roles this employee should not have	The risk if the employee does both roles	The compensating controls you could put in place include

Authorize write-offs of customer accounts, customer credit memos or customer refunds	When the same employee is responsible for billing, has access to cash or deposits, and can also adjust customer accounts, adjustments can be used to conceal theft.
	
	If the accounts receivable clerk does not have access to deposits, then the risk is limited to having too much control over the collections process. For example, they might write off accounts that should have been in active collection.
		• Develop and enforce a collection policy that establishes expectations for the accounts receivable clerk:
		  ▫ Require supporting documentation for all account write offs, credits or refunds
		  ▫ Require secondary authorization for write offs, or for those exceeding a certain amount
		• Monitor collection efforts to ensure policy requirements are followed
		• Periodically review customer account adjustments for reasonableness and the presence of supporting documentation

Approve payment plans	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 accounts of customers on payment plans against the aging accounts receivable reports for reasonableness, and to ensure past due balances are legitimate and policies have been followed.

3. 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 3**. It is separate from other functions around payroll, such as positions that establish wage rates, approve payroll payments, and issue or distribute payroll checks.

Diagram 3 – Payroll

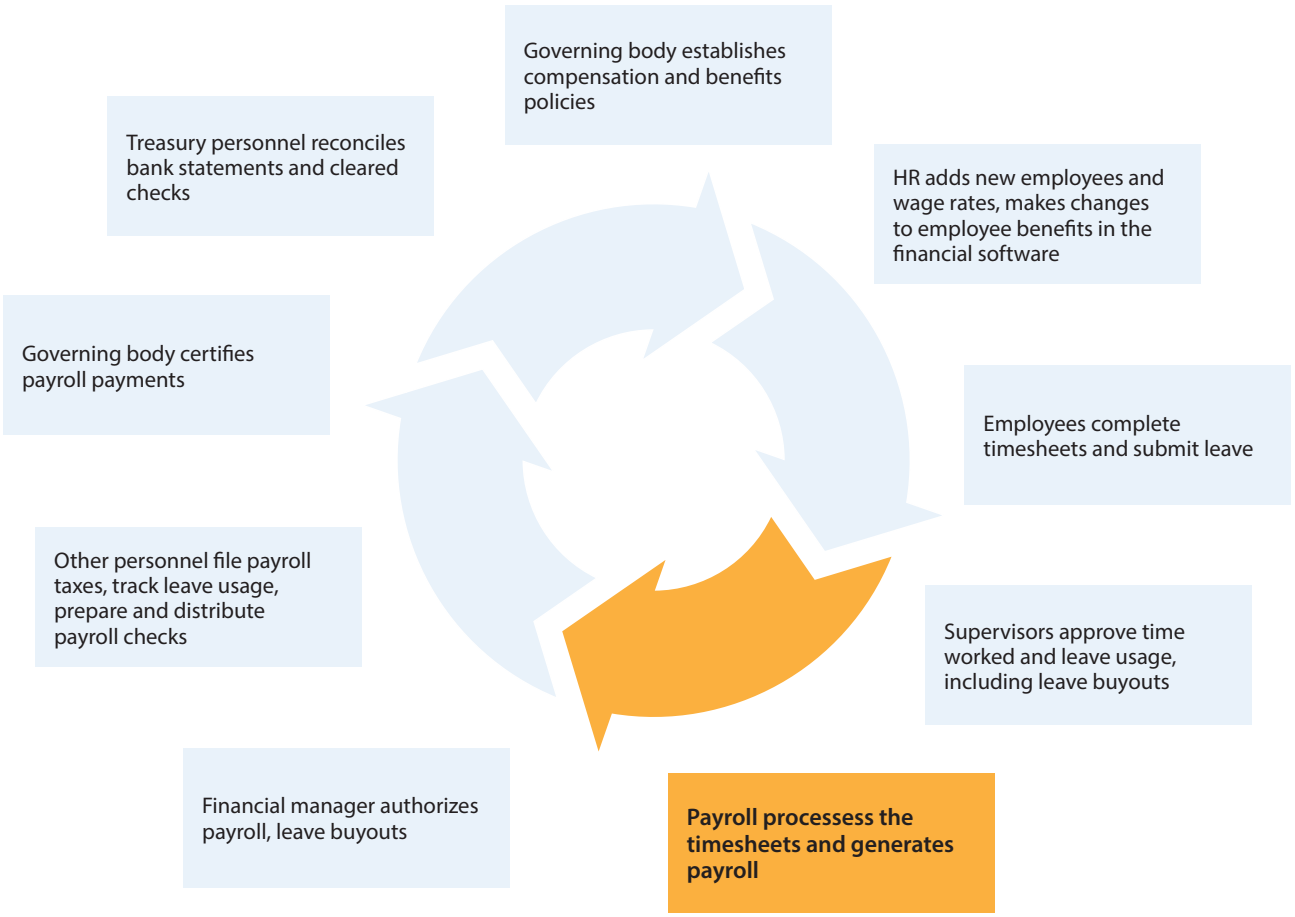


Table 3 – If the employee's job is to process payroll payments (typically called a payroll clerk), then:

Other roles this employee should not have	The risk if the employee does both roles	The compensating controls you could put in place include
Edit personnel master file, including the ability to add new employees, change wage rates or compensation, or change bank routing information for direct deposits.	**It becomes easier to create ghost (fictitious) employees to divert funds to a personal account**. A related scheme converts a terminated employee's record into a fake ongoing payee by changing bank routing information. **Note:** The risk of ghost employees rises if your software configuration allows the payroll clerk to approve or process unapproved timesheets. Increasing personal compensation for self, friends, family, or in collusion with another employee	• Review a weekly report of any changes made within the payroll system • Periodically review employee addresses and bank account numbers to determine if multiple payments are going to the same address or bank account. Verify requests to change a street address to a P. O. box. • Periodically compare a report of paid employees and wage rates to personnel files, including confirming terminated employees • If the final payroll register has been prepared by one person with these conflicting duties, pay special attention to issues in this list when you conduct the detailed review of payroll. • Set a policy requiring managers to regularly review their employee payroll reports
Approve time sheets or process unapproved time sheets	Increasing personal compensation for self, friends, family, or in collusion with another employee	• If the final payroll register has been prepared by one person with these conflicting duties, pay special attention to issues in this list when you conduct the detailed review of payroll • Set a policy requiring managers to regularly review their employee payroll reports
Generate payments or have access to checks	**Processing unauthorized payroll payments**. When the same employee responsible for producing payroll can also generate checks, it is easier to alter the payee name or deposit the checks directly into a personal account (such as for a fictitious employee).	• Consider outsourcing payroll payment generation and distribution, as well as payment of payroll taxes, to a payroll processing company. • Eliminate paychecks as much as possible by requiring employees to sign up for direct deposit, and ensure payroll staff cannot change routing information for direct deposits. • Secure the check stock until the day and time scheduled for payroll staff to produce paychecks • Review endorsed paychecks, preferably received directly from the bank, for alterations or unauthorized payments • Consider using your bank's Positive Pay service to detect check alterations. Reverse Positive Pay might also be an option. • Use a separate bank account (called a clearing account) for payroll payments to limit the funds available for payroll payments.

Table 3 – If the employee's job is to process payroll payments (typically called a payroll clerk), then:

Other roles this employee should not have	The risk if the employee does both roles	The compensating controls you could put in place include
Generate payments or have access to checks, *continued*	**Process unauthorized payroll payments**	• Reconcile the payroll clearing account to make sure only the appropriate amount of payments were withdrawn
Authorize payroll payments or be able to sign checks on the bank account	**Execute unauthorized payroll payments**	**Note:** We strongly advise local governments not to give both these roles to the same person. • If it is unavoidable, at a minimum, an independent person should periodically review payroll payments to ensure they are for genuine government employees. • Conduct a thorough background check and purchase a bond to cover this person's activities • Use two-signature authorizations on payroll checks. However, some banks will not monitor for this and you will need to consider other controls.
Reconcile bank accounts	When the same employee processes payroll and reconciles bank accounts, it is easier to make and conceal unauthorized payments	• Periodically review banking activity online or by requesting a copy of the bank statement directly from the bank • Compare bank statements and endorsed checks returned directly from the bank for irregularities • Periodically perform a secondary review of the bank reconciliation • Periodically have an independent person perform the reconciliation in its entirety • Outsource the bank reconciliation to an independent reviewer
Authorize leave buyouts, and also track leave usage for all employees (including self)	When a payroll clerk can also process leave buyouts, it is easier to add unauthorized payments. A payroll clerk that can adjust all leave might not record their own leave accurately.	• Monitor leave buyouts and review supporting documentation to ensure they comply with policy and were authorized • Monitor the payroll clerk's leave use and balances
Make changes to employee benefits	The payroll clerk might allow health care benefits to non-qualifying persons he/she is connected with (such as a spouse after divorce) or make additional contributions for retirement purposes for personal benefit.	• Periodically review supporting documentation for health benefits and retirement benefit payments to ensure they are correct

4. 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 4**. It is separate from other functions such as roles that authorize payments, issue/mail checks, or reconcile the bank account.

Diagram 4 – Accounts payable roles

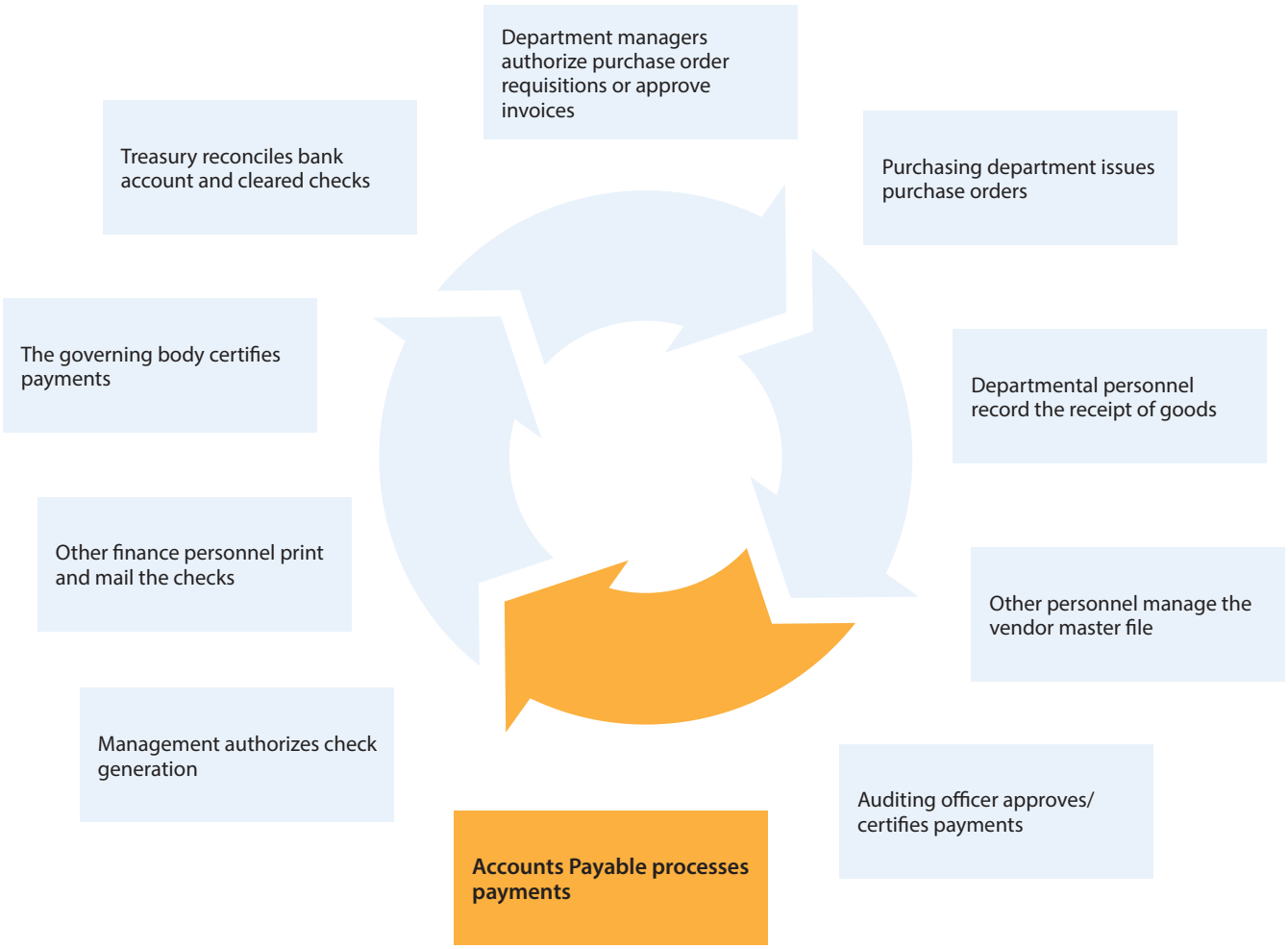


Table 4 – If the employee's job is to process vendor payments (typically as an accounts payable clerk), then:

Other roles this employee should not have	The risk if the employee does both roles	The compensating controls you could put in place include
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. A variation redirects payment for a legitimate vendor to the clerk's own address or bank account.	• Require management approval to set up new vendors or to make changes to existing vendors • Verify new vendors are legitimate businesses before approving set up • Periodically review a financial system report for any changes to vendor information and verify it is correct • Periodically compare employee addresses and phone numbers to those of vendors • Periodically evaluate that the vendor's efforts to carry out contracted work match expectations • When approving payments, monitor for and follow up on new or unfamiliar vendors, or those with unfamiliar "ship-to" addresses.
Generate payments or have access to checks	**Process unauthorized payments** **Check alteration schemes** – Modifying checks, such as altering the payee, or depositing the checks directly into a personal account	**Note**: We strongly advise local governments not to give both these roles to the same person. • Consider contracting with another suitable government or service provider, such as the county or an educational service district, to generate payments made on your accounts • Secure the check stock until accounts payable is ready to print checks, and then only provide enough to print the number of checks authorized • Review authorized check runs carefully to ensure there are no unaccounted-for gaps in the check sequence • Assign someone other than the accounts payable clerk to mail all checks • Review endorsed checks, preferably received directly from the bank, for alterations • Consider using your bank's Positive Pay service to detect check alterations. Reverse Positive Pay might also be an option. • Use a separate bank account (called a clearing account) for accounts payable payments to limit the funds available for making authorized payments.

Table 4 – If the employee's job is to process vendor payments (typically as an accounts payable clerk), then:

Other roles this employee should not have	The risk if the employee does both roles	The compensating controls you could put in place include
Serve as the auditing officer	When the same employee can process payments and conduct audits of the payment system, it is easier to conceal unauthorized payments	**Note**: We strongly advise local governments not to give both these roles to the same person. • If it is unavoidable, at a minimum consider transferring the oversight responsibilities of the auditing officer to someone else, such as an elected official or a contractor • Consider establishing a financial oversight subcommittee of the governing body to review all payments before sending out checks • Do not allow payments to be processed before the governing body approves them
Authorize payments in any form, including checks, electronic funds transfer and wire transfer, or otherwise serve as a signer on any of the government's accounts	When the same employee can both process and authorize payments, it is possible to make unauthorized payments.	**Note**: We strongly advise local governments not to give both these roles to the same person. • If it is unavoidable, at a minimum perform a secondary review of payments to ensure payments are for valid government purposes. • Conduct a thorough background check and purchase a bond to cover this person's activities • Use two-signature authorizations on all checks. However, some banks will not monitor for this and you will need to consider other controls. • Require a secondary authorization for electronic funds and wire transfers, at least above a specified threshold • Do not allow payments to be processed before the governing body approves them • Periodically review banking activity online or by requesting a copy of the bank statement directly from the bank
Reconcile the bank account or clearing account	When the same employee processes accounts payable and reconciles bank accounts, it is easier to make and conceal unauthorized payments	• Perodically review banking activity online, or by requesting a copy of the bank statement directly from the bank for unusual activity. Review endorsed checks as part of this monitoring process for any irregularities. • Perform a secondary spot-check review of the bank reconciliation • Outsource the bank reconciliation to an independent reviewer • Periodically have an independent person perform the reconciliation in its entirety

Table 4 – If the employee's job is to process vendor payments (typically as an accounts payable clerk), then:

Other roles this employee should not have	The risk if the employee does both roles	The compensating controls you could put in place include
Participate in cash receipting functions	An accounts payable clerk with the ability to write checks and also receive cash, can issue checks to back-fill shorted deposits. In other words, cash could be withdrawn from the deposit and the government's own check substituted for stolen cash.	• Thoroughly review accounts payable payments • Periodically review the composition of a deposit right before it is taken to the bank. For example, look for checks other than those from customers. • Check the deposit records to ensure cash/check composition agrees with what is recorded in the cash-receipting system

5. Purchasing and procurement

Of the multiple people who may be involved in procuring goods or services for a local government, the procurement or purchasing department is usually responsible for both vendor selection and negotiations, as well as issuing purchase orders and contracts. Their roles are shown in the orange box in **Diagram 5**. They are separate from other roles, such as taking custody of the goods or processing payments to vendors.

Diagram 5 – Purchasing system roles

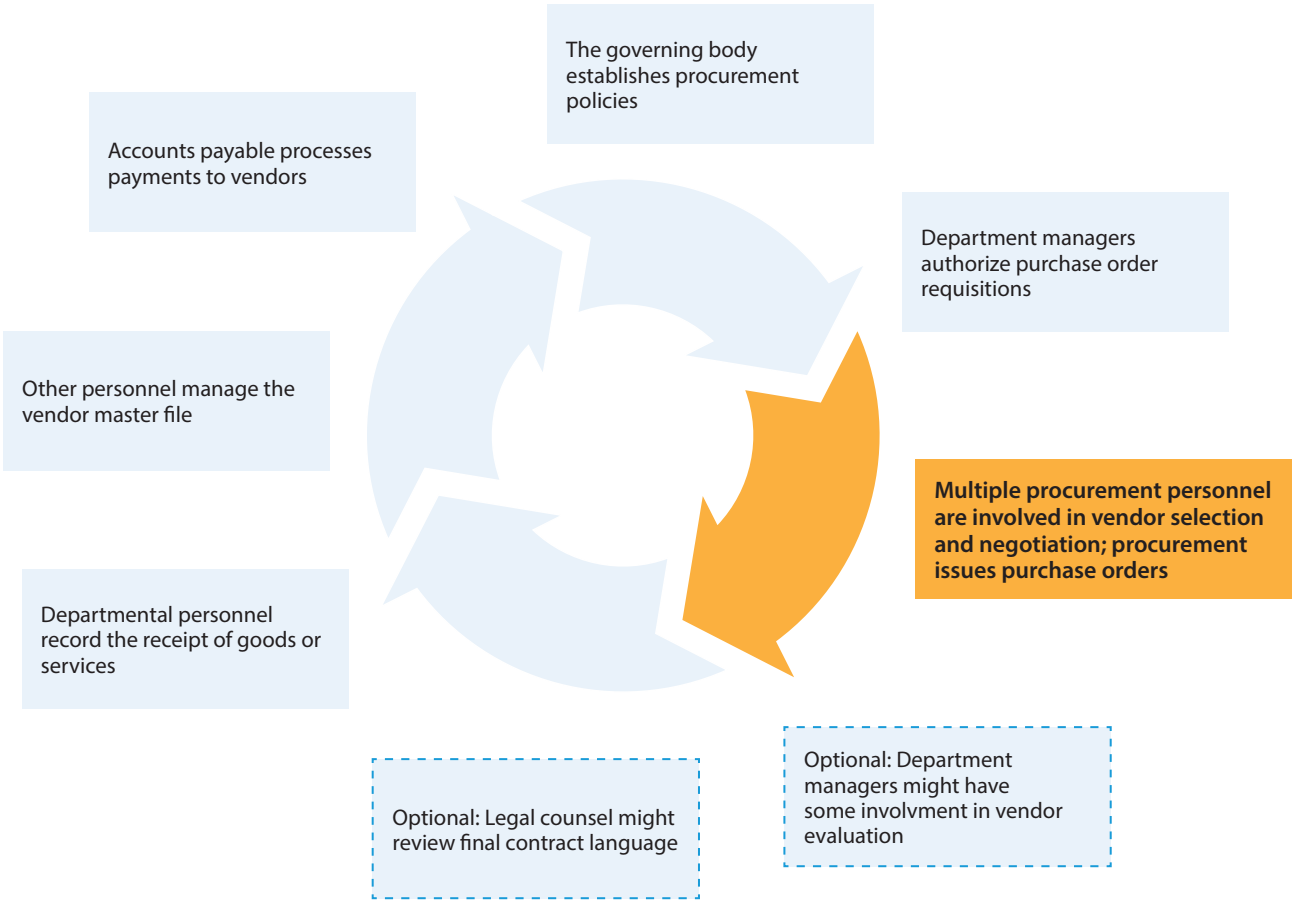


Table 5 – If the employee's job is to purchase or procure goods and services from vendors, then:

Other roles this employee should not have	The risk if the employee does both roles	The compensating controls you could put in place include
Create new vendors in the financial software	**Fictitious vendor schemes**. When the same employee can both purchase goods or services and enter a new vendor in the financial system, it is easier to create a fake business using a personal bank account, and "purchase" nonexistent products. The fake business might even use a legitimate vendor's name with a false pay-to account.	• Require management approval to set up new vendors or to make changes to existing vendors • Verify new vendors are legitimate businesses before approving set up • Periodically review all changes to vendor information using a system report if one is available • Periodically compare employee addresses and phone numbers to those of vendors • Periodically evaluate that the vendor's efforts to carry out contracted work match expectations • When approving payments, monitor for and follow up on new or unfamiliar vendors, or those with unfamiliar "ship-to" addresses
Enter and process payments in the accounts payable system	**Fictitious vendor schemes**	• When approving payments, monitor for and follow up on new or unfamiliar vendors, or those with unfamiliar "ship-to" addresses
Negotiate contracts without oversight or involvement by other personnel	**Kickback schemes**. An employee is bribed with cash, gifts or other forms of enticement in exchange for awarding a contract to the vendor, potentially without inviting competing bids or at unfavorable pricing.	• Perform a secondary review of contracts, considering the selection process, terms and vendor performance • Evaluate pricing of goods and services for reasonableness, and monitor for significant price increases that appear unfavorable to the government • Establish a procurement policy setting out steps employees must take to ensure they receive the best price. Policies should encourage competitive bidding or obtaining multiple quotations. • Establish a code of ethics policy for vendors and share it with them, such as on a schedule (once a year) or included in bid packets for significant procurements. • Periodically review a report of new vendor activity and ensure they are valid vendors
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 that received goods arrived and are on-site • Review purchase activity for reasonableness, nature and frequency of purchases • Establish a policy for tracking "small and attractive" assets

6. Inventory

The employee tasked with looking after inventory is managing consumable goods and equipment. Depending on your local government's role, inventory might encompass vehicle parts and supplies for a county repair shop, hospital supplies or pharmaceuticals, or copper and steel building materials for a public utility district. The orange box in **Diagram 6** shows the position of the person directly managing inventory; this role is separate from authorizing purchases, recording the initial receipt of goods, and making adjustments to inventory levels. However, not many government hold inventories of a size to warrant segregating these duties; the controls we suggest here are intended to compensate for your biggest risks.

Diagram 6 – Inventory system roles

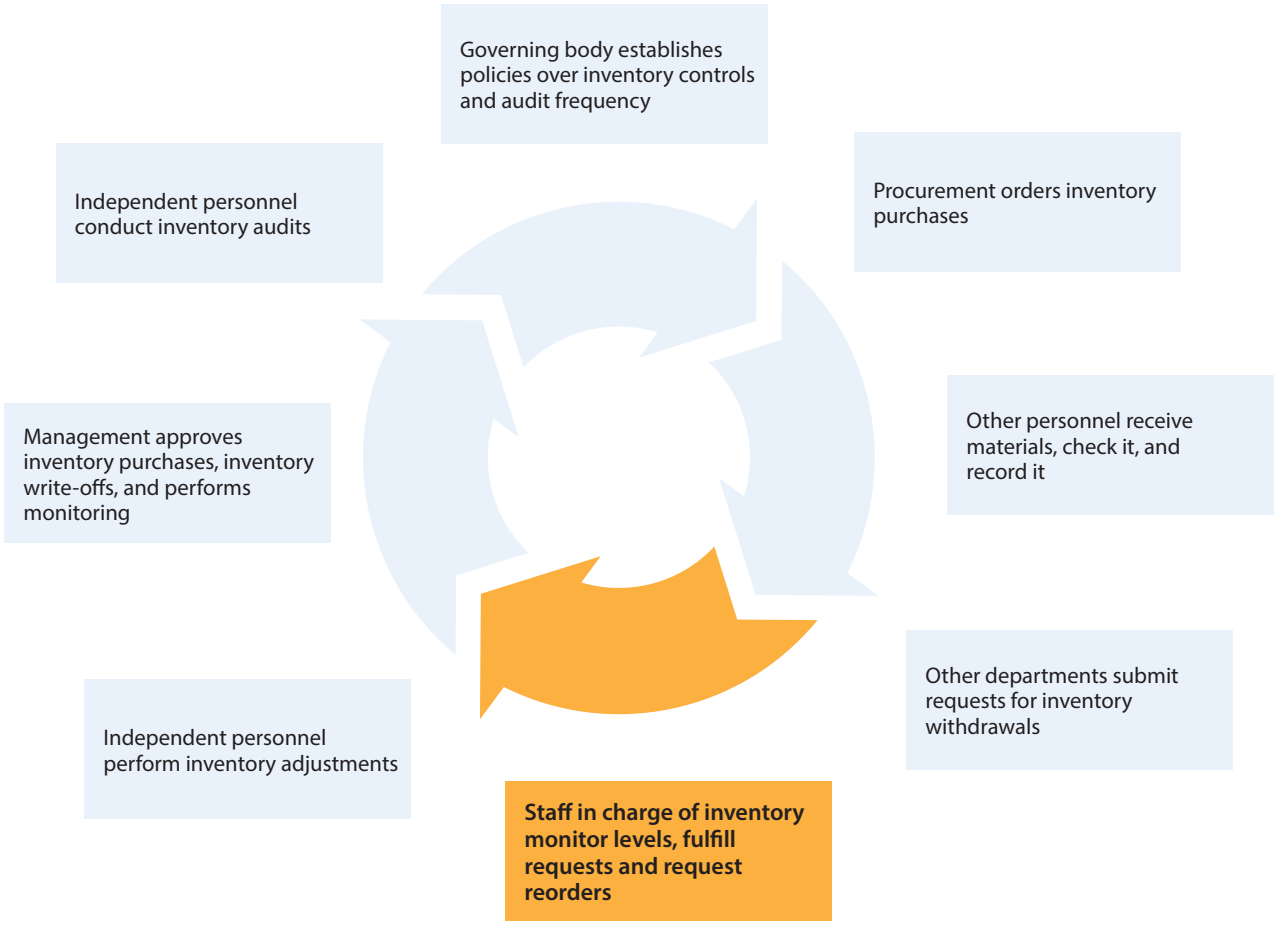


Table 6 – If the employee's job is to be responsible for/in charge of consumables or equipment held in inventory stores, then:

Other roles this employee should not have	The risk if the employee does both roles	The compensating controls you could put in place include
Purchasing	When the same employee purchases consumables and is responsible for managing them, it is easier to order extra stock and convert it to personal use.	• Review inventory purchases for unreasonable frequency or amounts
Receive and record inventory	When the same employee can record items as received and manage the quantity of stock, it is easier to disguise quantities by not recording them upon receipt, in turn making theft easier to hide.	• Periodically conduct independent spot-checks that ordered items were received and recorded in inventory records, specifically include in the spot check some valuable or high risk items
Adjust inventory levels	Stock can be stolen and the act concealed by adjusting inventory records.	• Require documentation of inventory adjustments, including for quantity adjustments and other write-offs • Set authorization levels appropriately, including the option of two-person approvals for significant adjustments • Periodically review the adjustment activity for reasonableness
Conduct inventory counts or audits	Inventory might be missing but no one is alerted.	**Note**: We strongly advise local governments not to give both these roles to the same person. • If it is unavoidable, at a minimum review the inventory and spot-check some items • Periodically conduct independent surprise inventory counts, especially for valuable and high risk items • Review system reports for incorrect or unlikely results, such as items with negative inventory balances, and follow up
Authorize inventory distributions or withdrawals	When the person responsible for maintaining inventory stocks can also authorize distribution of stock, it is easier to disguise improper withdrawals from stock.	• Require supporting documentation for inventory withdrawals to ensure they are both reasonable and valid

Table 6 – If the employee's job is to be responsible for/in charge of consumables or equipment held in inventory stores, then:

Other roles this employee should not have	The risk if the employee does both roles	The compensating controls you could put in place include
Scrapping or disposing of inventory (such as pharmaceuticals past expiration date or a type of wire that is no longer used in operations)	When the person responsible for maintaining inventory stocks is also in charge of disposing of unwanted goods, it is easier to convert them to personal use or sell them for personal gain.	**Note**: Compensating controls will vary based on the type and amount of inventory to be scrapped • Require documentation for scrapped inventory, including two-person certification for how it was disposed of • Monitor the value of scrapped inventory to ensure it meets expectations for normal business patterns • Monitor scrap revenues, if the items are metal and sold for scrap

7. Capital and other valuable assets

The employee tasked with looking after capital assets is managing durable goods that you likely expect to be safeguarded, accounted for, and only used in the government's operations. Depending on your local government's role, capital assets might include "small and attractive" items like computers, cell phones, heavy equipment or vehicles. The orange box in **Diagram 7** shows the position of the person managing capital assets. This employee's role is separate from authorizing purchases, updating the tracking system for changes, and handling the sale or surplus of assets.

Diagram 7 – Capital and valuable assets roles

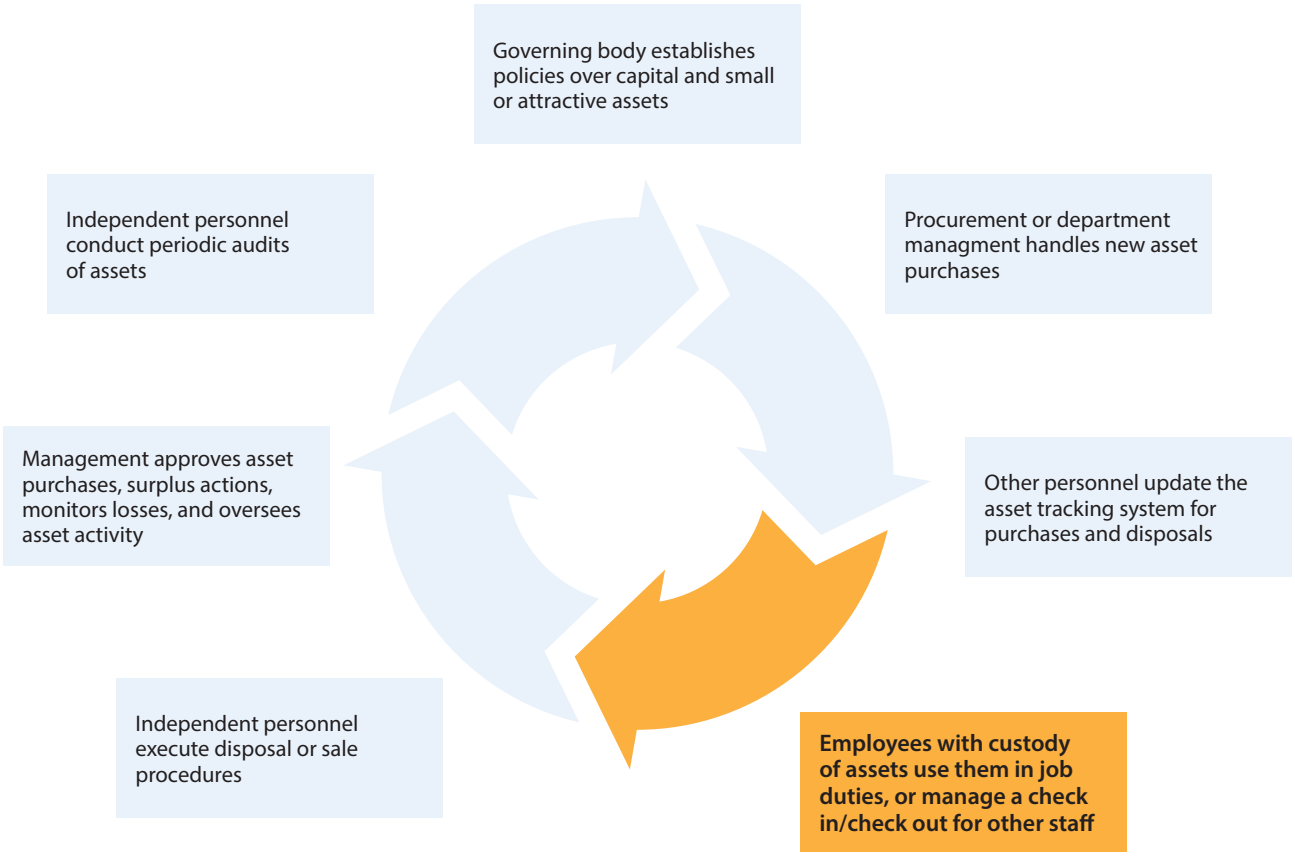


Table 7 – If the employee's job is to be physically responsible for capital or other valuable assets, then:

Other roles this employee should not have	The risk if the employee does both roles	The compensating controls you could put in place include
Authorize purchases	When the same employee can authorize a purchase and is responsible for managing the item, it is easier to order extra or unneeded equipment and convert it to personal use.	• Periodically assess purchasing activity to see if it is reasonable • Establish a system to track assets upon purchase • Periodically conduct an internal audit of the asset-tracking system • Periodically spot-check that purchases arrived at the correct address and are on site • Establish a central file to hold titles for assets such as vehicles
Record the asset on an asset-tracking and/or accounting system	The purchase might not be recorded on the asset tracking system in order to conceal a misappropriation.	• Periodically spot-check that assets have been properly recorded using recent purchasing records
Modify the asset-tracking system and/or accounting system	When the same employee can modify the quantity or details of purchased asset, it is easier to conceal misappropriation by deleting records from the tracking or accounting system.	• Periodically review deleted records from the asset tracking or accounting system • Periodically trace purchases from purchase order through the tracking system to ensure all assets are recorded properly
Conduct all tasks involved in disposing of assets, including: • Authorizing disposal • Making arrangements for the sale or disposal • Physically execute the sale as the last person responsible for the item	When the same employee has custody of capital assets and can arrange for their disposal, it is easier to take the proceeds from the sale or use the money for unallowable purposes, or to convert discarded items to personal use.	• Establish clear policies concerning surplus procedures and ethical expectations of employees If employees may purchase surplused items, ensure the policy states how they may do so. • Set up a central monitoring system to ensure asset disposals are tracked and funds are received • Require that supporting documents, such as bills of sale, are retained in the central system • Establish a secure, central file to hold titles for assets such as vehicles • Set up a two-person approval system so that capital asset sales can't be executed by one person • Periodically spot-check new capital purchases to ensure the items that previously performed the function were disposed of properly.

Table 7 – If the employee's job is to be physically responsible for capital or other valuable assets, then:

Other roles this employee should not have	The risk if the employee does both roles	The compensating controls you could put in place include
Conduct internal audits of capital assets	When the same employee has both custody of assets and is responsible for accounting for their whereabouts, it is easier to disguise theft or loss.	**Note**: We strongly advise local governments not to give both these roles to the same person. • If it is unavoidable, at a minimum spot-check internal audits to ensure they have been done properly. • Periodically trace purchases from purchase order through the tracking system to ensure all assets have been properly accounted for.

8. 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 are occurring 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 8**. It is separate from other functions, such as those that cash receipt, process accounts payable or payroll payments, and – perhaps most importantly – people that can sign on the organization's bank accounts.

Diagram 8 – Banking system roles

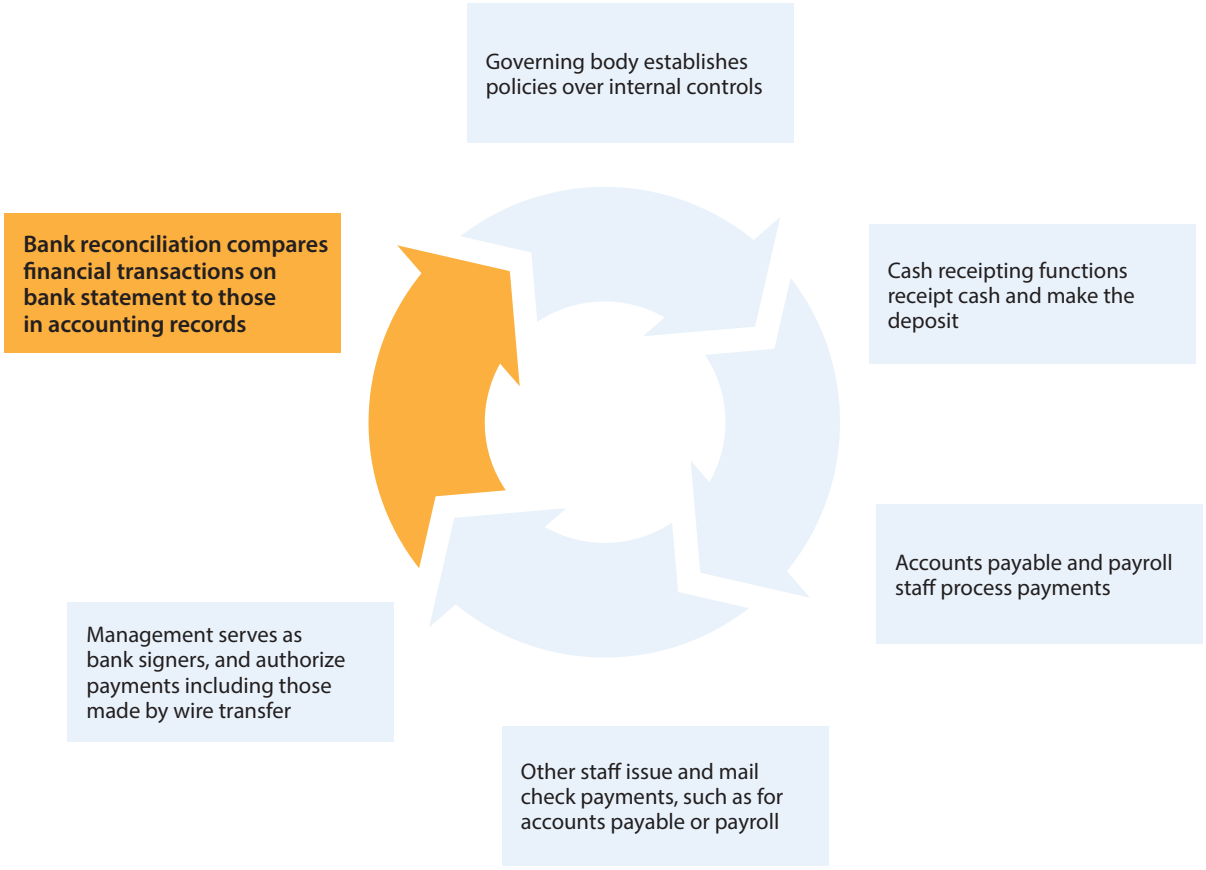


Table 8 – If the employee's job is to be responsible for reconciling the bank statement and its activity, then:

Other roles this employee should not have	The risk if the employee does both roles	The compensating controls you could put in place include
Access to the bank deposit, including having access to the safe	The bank deposit may be stolen or lost and the theft go undetected.	• Conduct a secondary review of the reconciliation to ensure deposits are accounted for and deposited
Process payroll or accounts payable payments	When the same employee can both process payments and reconcile bank statements, it is easier to conceal theft or loss.	• Review endorsed checks, preferably received directly from the bank, for alterations • Periodically review bank accounts online, or at least between monthly statements, to check for unusual activity • Ensure there are no gaps in check sequences for payments certified by the governing body • Perform a secondary review of the bank reconciliation • Periodically have an independent person perform the reconciliation in its entirety • Outsource the bank reconciliation to an independent reviewer
Be able to process or authorize electronic funds transfer or wire transfers or other electronic payments	When the same employee can both process and authorize electronic payments and reconcile bank statements, it is easier to make and conceal unauthorized payments.	• Establish a protocol with the bank to require a secondary approver for electronic payments or wire transfers • Impose a limit with the bank so that those authorized to send wires are limited in how much they can execute
Be an authorized signer on the government's bank account	Allows the employee to make withdrawals or transfers to other accounts without detection	• Review bank account activity, using online access or bank statements sent directly by the bank, for reasonableness and accuracy

9. General ledger

Accountants are responsible for recording transactions and making journal entries and other changes to the government's general ledger. They should not have access to assets or authorize the transactions for the journal entry that they prepare. Their role is shown in the orange box in **Diagram 9**. It is separate from other functions such as cash receipting and processing accounts payable or payroll payments.

Diagram 9 – General ledger system roles

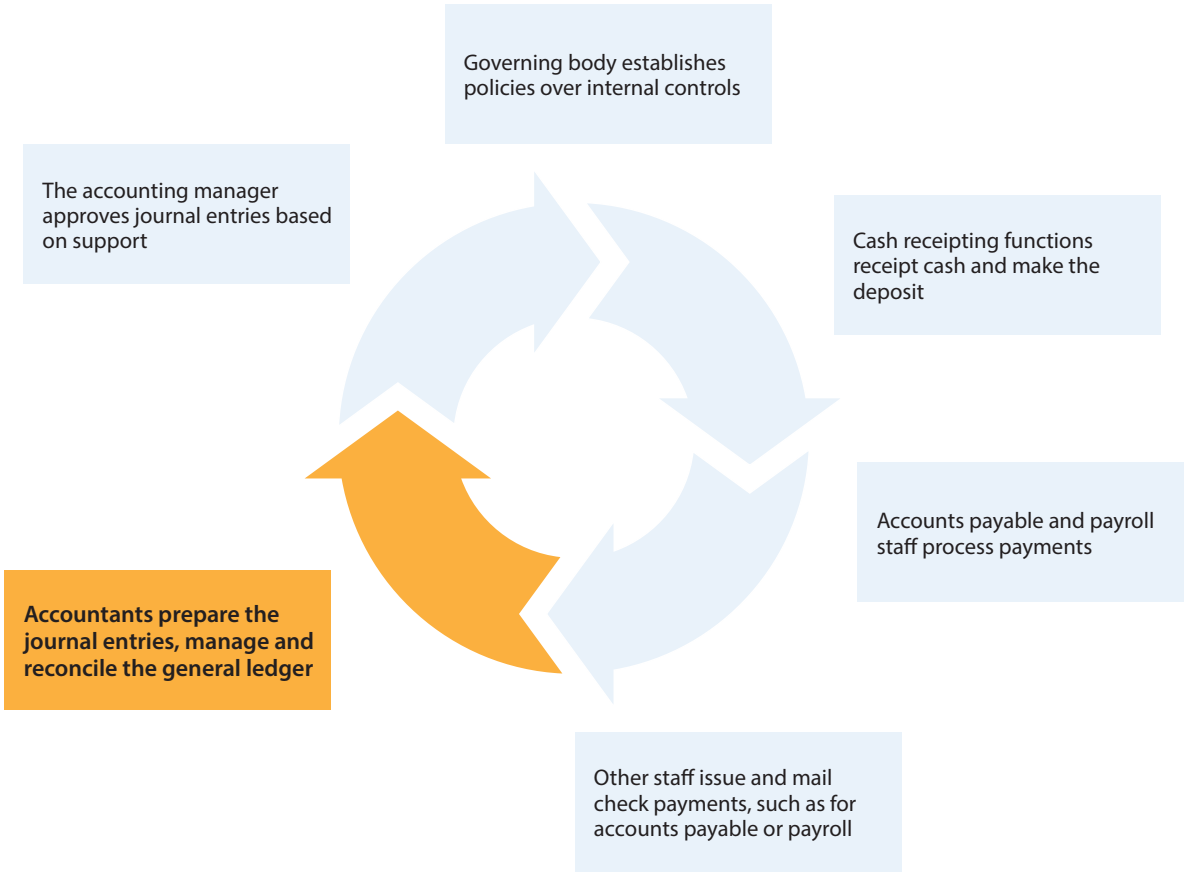


Table 9 – If the employee's job is to perform journal entries or make other changes to the general ledger, then:

Other roles this employee should not have	The risk if the employee does both roles	The compensating controls you could put in place include
Access to deposits or other funds and assets	When the same employee has access to money or assets and can also make journal entries, it is easier to move funds within the general ledger conceal theft or loss of funds.	• Require secondary review of each journal entry and its supporting documentation. Be alert to entries directly affecting cash or reclassifications of revenue or expense. • Periodically spot-check 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, it is easier to move funds within the general ledger conceal theft or loss of funds.	• Require secondary review of each journal entry and its supporting documentation. Be alert to entries directly affecting cash or reclassifications of revenue or expense. • Periodically spot-check for unusual journal entries and follow up
Prepare and approve a journal entry	When the same employee both enters and approves journal entries, 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. • Consider contracting with an external reviewer if no one within staff or the governing body has the knowledge or ability to review journal entries. • Consider partnering with a neighboring government to help each other monitor certain tasks such as journal entries.

Section 3 – Information Technology: Aligning software user access with duties

Local governments can separate employee duties in practice but it might not actually reduce risk if they do not also restrict access to the related software applications and systems. You can do this most easily by setting up appropriate user access or permissions in your financial software. For example, the payroll clerk should not have the ability to add new employees to the payroll system, which means the clerk should not have access to that function within the software. Employees should have the minimum system access they need to perform their job duties and nothing more.

Leading practices recommend that no one employee be able to initiate, process, post, adjust and approve a transaction within a system. If you separate duties properly, and align user access permissions with those assigned duties, you can achieve a significant reduction in risk. Establish a process for setting user access that includes regularly reviewing those permissions and you can reduce risk even further.

What to look out for

The most common risk points include:

- Employees are given full access to software features, such as editing an entry, when read-only access is sufficient to perform their jobs.
- Employees and managers are given full access in case they might be asked to fill in during a colleague's vacation or sick leave.
- Employees transitioning between departments and job responsibilities retain access to wrap up old projects, but also gain additional access for new duties. Once given, the access for their previous job might not be re-evaluated for some time – or at all.
- During new system implementations, employees are given full access while they familiarize themselves with the system and how it functions. Again, once given, the permission levels might not be reviewed and adjusted for some time.
- Software might not allow customization of user access permissions, effectively having an "all or nothing" functionality.

If you can't configure your financial system's user access profiles to reduce the risks, then you will need to choose and implement one or more of the compensating controls in this guide to help detect problems if they arise.

Steps you can take to reduce risk related to software and information technology (IT) systems

At the most basic level, this list of best practices outlines what experts advise small local governments to do in order to reduce the risk that financial, accounting and other types of computer software will be misused. Read below the list for ideas about on how to put them into action.

1. Align software access and permission levels with job duties, which means to the least access they need to do their job duties.
2. Assign users "read-only" access when viewing transactions is sufficient to do their job.
3. Ensure the IT department manages all user permissions for all software systems you use.
4. Limit administrative access to software systems– even within the IT team – as much as possible.
5. Do not grant employee or manager access to software for sick-leave or vacation cover until it is actually needed.
6. Regularly monitor and review user permissions on a routine basis, at least annually.
7. Manage user permissions during a new system implementation, and review as promptly as possible afterwards.
8. Develop and implement policies and procedures to manage user permissions.

The policy should set out procedures your office can follow to act on your IT access policies

The policies you develop around financial software do not have to be long or complex to be effective. At a minimum, though, it should address two essential issues: when to review user access and who is responsible for managing user access. The policy might also require the use of forms to document the approval process for changes to user access. In fact, these policies should apply to all software your office uses. An ex-employee who can still log in to email or network folders increases risk to data and information you don't want exposed.

When to review user access

Your financial software policy should set out the circumstances, timing and frequency of software reviews. Experts recommend these timings:

- At least annually
- When software or systems are updated with new versions or security patches
- When new employees are hired or existing employees move to another role in the organization
- When employees leave your office

Who should manage user access

Most small governments have limited approaches to managing financial software, and which you choose will likely be driven as much by staffing as by the desire to follow best practices.

If you have an IT department or a dedicated employee. Best practice recommends assigning an IT specialist with no conflicting duties in finance to manage user-access rights and permissions within financial software applications. Your policy should spell out that the IT specialist coordinate with finance or other departments to understand the job duties associated with user-access levels in the software, and restrict employee access as appropriate.

If you lack an IT specialist but have software expertise within the department that uses it. Some governments choose to use this approach even if they have an IT specialist, on the grounds that the department best understands the job duties of its personnel. However, the department may find it very difficult to fully separate conflicting duties or provide adequate oversight to reduce risk. Specifically, it opens the door for administrative users to initiate, process, post, adjust or approve their own transactions, and to change and manipulate transactions or other user profiles, without proper oversight. If you choose this strategy, you will need to create compensating controls to address any risks the decision can create, although it might be challenging to do so.

If an elected official or board member has relevant IT expertise. A third option is to seek the help of the governing body. Because they are unlikely to work in the day-to-day transactions of financial systems, they may be in a good position to adjust user access permissions without compromising your system of controls. But be sure their experience is truly relevant: adjusting user access is not necessarily as simple as installing Microsoft Office on a new PC.

If you have sufficient funds to pay an outside expert. Budgeting for an annual review of your IT system health and user access permissions may be a very workable alternative to managing these tasks in-house – especially if doing so eliminates a significant portion of conflicting duties.

Appendix A – Example of duty assignments for small governments

One-person accounting department

Strong oversight and independent authorization of transactions are essential if you must function with a one-person accounting department. Innumerable risks arise when one person is given so many duties and responsibilities. To adequately mitigate risk, you will need at least one other person to provide oversight. Among your options:

- An elected official or member 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 they are looking for. (A quick review of the Risks column in the detailed sections of this guide can help.) And finally, don't rely on an audit to discover fraud or verify it isn't taking place. Every local government is responsible for safeguarding its assets before something happens. **Figure 1** illustrates one way duties might be separated in a one-person accounting department.

Figure 1: One way to organize a one-person department

Duty (and related page)	Clerk 1	Oversight person
Cash receipt (p. 10)	Collect receipts from customers, prepare the deposit, and make the deposit with the bank	Ensure deposits were made intact by comparing paper receipt records (source records to support the deposit) to bank statement deposit information. This should include confirming that cash vs. check composition is correct for all deposits.
Accounts receivable (p. 15)	Send out billings, post payments to accounts, perform collections	Monitor key reports including aging reports, monthly revenue activity, and adjustments to customer accounts
Payroll (p. 18)	Process and prepare checks (or use a 3rd party vendor or County Auditor if possible)	Review the payroll register, approve time sheets, sign and distribute checks
Accounts payable (p. 21)	Process invoices and prepare checks (or use County auditor)	Review supporting documentation, approve invoices, sign and mail checks
Purchasing and procurement (p. 25)	Obtain or review quotes or bids	Review and sign all contracts or purchase orders
Capital assets (p. 30)	Maintain a listing	Periodically check to ensure all assets are accounted for (inventory) and used for governmental purposes
Banking (p. 33)	Prepare the bank reconciliation	Be the signer on the account. Review the bank reconciliation. Monitor banking activity with direct online access or by having an original statement mailed directly with the copies of endorsed checks.
General ledger (p. 35)	Perform journal entries	Review and approve

Two-person accounting department

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

- An elected official or member 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 they are looking for. (A quick review of the Risks column in the detailed sections of this guide can help.) **Figure 2** illustrates one way duties might be separated in a two-person accounting department.

Figure 2: One way to organize a two-person department

Duty (and related page)	Clerk 1	Clerk 2	Oversight person
Cash receipt (p. 10)	Perform receipting, prepare the deposit, and deliver the deposit to the bank (if needed)	Backup cash receipt, but limit access as much as possible to all receipts and the deposit	No access. Might do a last look at the deposit periodically to ensure checks deposited are only that of customers.
Accounts receivable (p. 15)	No duties	Send out billings, manage customer accounts, collections, customer concerns	As clerk 2 will likely be a backup to cash receipt, additional oversight over accounts receivable key reports such as account adjustments
Payroll (p. 18)	Edit the payroll master file, preliminary review of the payroll register, and prepare checks	Process the payroll	Final review of the payroll register and payroll payments, authorize pay increases
Accounts payable (p. 21)	Process invoices, prepare checks	Edit vendor master file	Final review and authorize payments
Purchasing and procurement (p. 25)	No duties	Obtain and review bids	Review and approve purchase over a certain threshold
Capital assets (p. 30)	Maintain a listing	Periodically conduct an inventory	Optional review of the inventory and listing
Banking (p. 33)	None	Reconcile the bank activity	Be the signer on the account. Review the bank reconciliation in detail, ensure deposits are made intact if clerk 2 has any access to the deposit (prevent if possible).
General ledger (p. 35)	Prepare journal entries	Review	Optional review

Three-person accounting department

Compared to one- and two-person departments, risks start to decrease significantly in a three-person operation. Conflicting duties can be more readily distributed between three, with more opportunities to rotate duties periodically to strengthen controls. Oversight is still needed and plays a key role, but the transactions that person is authorizing pose fewer risks and the review procedures can be less extensive. **Figure 3** illustrates one way duties might be partially separated with a three-person accounting department.

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

Duty (and related page)	Clerk 1	Clerk 2	Clerk 3	Oversight person
Cash receipt (p. 10)	Receipt cash from customers and take the deposit to the bank	Backup cash receipt, but limit access as much as possible to all receipts and the deposit. Prepare the deposit.	Monitor to ensure the deposits are made by comparing validated bank receipt to source records	No duties or access to the deposit
Accounts receivable (p. 15)	No duties	Post payments to customer accounts, send out billings	Execute any account adjustments, approve under a threshold	Approve write offs or refunds over a certain threshold
Payroll (p. 18)	Add new employees and wage rates	Process time sheets and prepare/mail payroll checks	Review the payroll register and file payroll taxes	Approve time sheet, pay increases, authorize payroll payments
Accounts payable (p. 21)	Process invoices and prepare/mail the checks. Prepare any electronic payments.	Edit vendor master file – add new vendors	Serve as auditing officer	Authorize invoices and checks and any electronic payments. Review the bank reconciliation.
Purchasing and procurement (p. 25)	No duties	No duties	Obtain and review bids	Review and approve purchase over a certain threshold
Capital assets (p. 30)	Maintain a listing	Option to review the listing and inventory	Conduct an inventory	
Banking (p. 33)	No duties.	No duties	Reconcile the bank activity	Be the signer on the account. Review the bank reconciliation in detail, ensure deposits are made intact if clerk 2 has any access to the deposit (prevent if possible).
General ledger (p. 35)	Prepare journal entries	Prepare journal entries	Review	Option to review

Appendix B – Self-assessment checklist

How to use this checklist

This checklist is intended to help you assess risks posed by conflicting duties in your organization, and give you space to record which control you can apply to reduce those risks. Remember, in many cases the cautionary word in the checklist is "*can*." It means you should consider not only conflicting *assigned* duties, but also if the employee in question has the ability to access the conflicting task, whether or not it is part of his or her assigned duty.

You may need several compensating controls to reduce risk to an acceptable level. Furthermore, a control's effectiveness depends as much on its operation as on its design. For example, review procedures are often a compensating control, but to be effective, reviewers must be diligent, thorough, know and understand the risk(s) they are reviewing for, and be prepared to follow up when they notice irregularities.

It can be difficult to conclude with confidence that the compensating controls you have selected are effective without substantial effort and testing. Even if you can confirm a control is operating effectively, there is no guarantee it will continue to do so in perpetuity. Use your best judgment and knowledge of your control system and employees to select primary controls and to assess whether additional controls are warranted.

Legend to columns in the following tables

A = Are duties segregated? Yes/No. If No, go to next column, B.

B = What is management's risk tolerance level given the specific risk(s) created by the lack of segregation of duties? (VH=very high, H=high, M=moderate, L=low, VL=very low)

C = Describe the compensating controls in place to address the risks caused by lack of segregation of duties. These might be broad controls and/or specific controls that directly target the risk, or some combination thereof. Consider one or more of the possible specific controls cross-referenced in this guide.

D = In your judgment, do the compensating controls seem appropriate to reduce risk to meet the risk tolerance level documented in column B? Yes/No. If No, go to the next column, E.

E = Describe some additional controls that might work to reduce risk to an acceptable level. Again, they might be specific, broad or a combination.

		A	B	C	D	E
Topic #	Topic area	Segregated (Y/N)	Risk	Compensating controls	Sufficient (Y/N)	Additional controls
1	**Cash Receipting – page 10** (Note: Complete for each cash receipting operation)					
1a	Do cashiers have complete control over issuing receipts? For example, could they issue an unauthorized receipt or not give a customer a receipt and pocket the money undetected?					
1b	Can cashiers also void receipts or process refunds to customers?					
1c	Do cashiers who receipt in-person cash or check payments also open payments that come through the mail?					
1d	Can cashiers generate or modify the billings for goods or services?					
1e	If applicable, do cashiers accept cash and also admit entry (such as into an event or parking)?					
1f	Can cashiers, or others with access to the deposit, adjust customer accounts?					

		A	B	C	D	E
Topic #	Topic area	Segregated (Y/N)	Risk	Compensating controls	Sufficient (Y/N)	Additional controls
1g	If accepting payment for goods, can cashiers perform inventory adjustments?					
1h	Do cashiers also apply the payments to customer accounts?					
1i	Do cashiers also prepare the deposit?					
1j	Do cashiers also take the deposit to the bank?					
1k	Do cashiers, or those with access to the deposit, perform the reconciliation of the deposit source records (receipts, system reports) to validated bank receipts?					
1l	Do cashiers, or those with access to the deposit, perform the reconciliation of the respective bank account(s)?					
1m	Do cashiers, or those with access to the deposit, participate in accounts payable functions?					

		A	B	C	D	E
Topic #	Topic area	Segregated (Y/N)	Risk	Compensating controls	Sufficient (Y/N)	Additional controls
2	**Accounts Receivable (A/R) – page 15**					
2a	Do A/R staff perform cash receipting functions (including relief cashier responsibilities), or have access to the deposit, or have access to the safe holding the deposit?					
2b	Can A/R staff modify billing rates in the software system, or otherwise edit or modify fees or charges in billings?					
2c	Do A/R staff write off and authorize customer account balances, or issue refunds or credits? (Note: Fraud risk increases if they also have access to the receipts or deposit.)					
2d	Do A/R staff approve payment plans? (Note: Fraud risk increases if they also have access to the receipts or deposit.)					
2e	Can A/R staff generate payments in accounts payable and also have access to the deposit?					

		A	B	C	D	E
Topic #	Topic area	Segregated (Y/N)	Risk	Compensating controls	Sufficient (Y/N)	Additional controls
3	**Payroll Processing – page 18**					
3a	Can payroll staff add new employees?					
3b	Can payroll staff change wage rates or compensation in the software system?					
3c	Can payroll staff change bank routing information for direct deposits for employees?					
3d	Can payroll staff process unapproved time sheets or otherwise approve time sheets?					
3e	Does anyone who can process payroll also generate payments, or otherwise access resulting checks?					
3f	Does anyone who can process payroll also authorize payments?					

		A	B	C	D	E
Topic #	**Topic area**	**Segregated (Y/N)**	**Risk**	**Compensating controls**	**Sufficient (Y/N)**	**Additional controls**
3g	Does anyone who can process payroll also serve as a signer on the bank account?					
3h	Does anyone who can process payroll also reconcile the bank account or clearing account?					
3i	Do payroll staff control the recording and tracking of leave (including their own), process leave buyouts, and also approve them?					
3j	Does any one person have complete control over changes made to health care or retirement benefit accounts?					

		A	B	C	D	E
Topic #	Topic area	Segregated (Y/N)	Risk	Compensating controls	Sufficient (Y/N)	Additional controls
4	**Accounts Payable – page 21**					
4a	Can staff who process invoices also add new vendors or modify existing vendor information?					
4b	Can staff who process invoices also generate payments/checks, or otherwise access checks after they are printed?					
4c	Does anyone who can process accounts payable invoices also authorize payments? (This might include serving as the auditing officer.)					
4d	Can staff who prepare checks, wire transfers or electronic payments authorize them?					
4e	Does anyone who can process accounts payable invoices also serve as a signer on the bank account?					
4f	Does anyone who can process accounts payable payments also reconcile the bank account or clearing account?					

		A	B	C	D	E
Topic #	Topic area	Segregated (Y/N)	Risk	Compensating controls	Sufficient (Y/N)	Additional controls
4g	Do staff who process accounts payable payments *and* have access to checks also participate in cash receipting functions or otherwise have access to the deposit?					

		A	B	C	D	E
Topic #	Topic area	Segregated (Y/N)	Risk	Compensating controls	Sufficient (Y/N)	Additional controls
5	**Procurement and Purchasing – page 25**					
5a	Are procurement staff restricted from accessing the accounts payable module, either to enter or change vendor information or to process invoices or payments?					
5b	Are procurement staff able to negotiate contracts without oversight (that is, be solely responsible for hiring certain vendors)?					
5c	Are procurement staff able to order goods and physically receive them upon shipment, or otherwise have custody?					

		A	B	C	D	E
Topic #	Topic area	Segregated (Y/N)	Risk	Compensating controls	Sufficient (Y/N)	Additional controls
6	**Inventory – page 27**					
6a	Do the same staff purchase and also receive/record the inventory in the records?					
6b	Can the staff with physical custody of the inventory adjust inventory levels?					
6c	Does the staff with physical custody of the inventory also perform the inventory count?					
6d	Does the staff with physical custody of the inventory also authorize inventory distributions or withdrawals?					

		A	B	C	D	E
Topic #	Topic area	Segregated (Y/N)	Risk	Compensating controls	Sufficient (Y/N)	Additional controls
7	**Capital and Other Valuable Assets – page 30**					
7a	Does the same staff purchase and take custody of the assets?					
7b	Does the same staff record the asset in the inventory tracking or accounting records and take custody of it?					
7c	Can the custodian modify the inventory tracking or accounting system that tracks the existence of the asset? For example, can they delete assets from the record?					
7d	Does the custodian authorize, manage or execute the disposal or sale of assets in their custody?					
7e	Does the custodian conduct audits of the assets they have control over and manage?					

		A	B	C	D	E
Topic #	Topic area	Segregated (Y/N)	Risk	Compensating controls	Sufficient (Y/N)	Additional controls
8	**Banking – page 33**					
8a	Does the person who performs the bank reconciliation also have access to the deposit, whether by taking it to the bank or having access to the safe?					
8b	Can the person who performs the bank reconciliation process payroll or accounts payable payments?					
8c	Can the person who performs the bank reconciliation send or authorize wire transfers or other electronic payments?					
8d	Is the person who reconciles the bank account also a signer on the bank account?					

		A	B	C	D	E
Topic #	Topic area	Segregated (Y/N)	Risk	Compensating controls	Sufficient (Y/N)	Additional controls
9	**General Ledger (Perform journal entries) – page 35**					
9a	Can preparers of journal entries receipt or deposit cash, or execute payments?					
9b	Do preparers of journal entries approve their own entries?					

Space for notes

Mission statement and State Auditor's Office contacts

The mission of the Office of the Washington State Auditor

To provide citizens with independent and transparent examinations of how state and local governments use public funds, and develop strategies that make government more efficient and effective.

The results of our work are widely distributed through a variety of reports, which are available on our website and through our free, electronic subscription service.

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
360-902-0360, Pat.McCarthy@sao.wa.gov

Kelly Collins – Director of Local Audit
360-902-0091, Kelly.Collins@sao.wa.gov

Kristina Swanson – Director of Innovation and Technology
360-753-0646, Kristina.Swanson@sao.wa.gov

Debbie Pennick – Assistant Director for the Center for Government Innovation
509-334-5825, x108, Deborah.Pennick@sao.wa.gov

Sherrie Ard – Center Program Manager
360-725-5552, Sherrie.Ard@sao.wa.gov

Kathleen Cooper – Director of Communications
360-902-0470, 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

1-866-902-3900

Office of the Washington State Auditor