Office of the New York State Comptroller

Division of Local Government and School Accountability

LOCAL GOVERNMENT MANAGEMENT GUIDE

The Practice of Internal Controls

Thomas P. DiNapoli State Comptroller

For additional copies of this report contact:

Division of
Local Government and School Accountability
110 State Street, 12th floor
Albany, New York 12236
Tel: (518) 474- 4037
Fax: (518) 486- 6479
or email us:
localgov@osc.state.ny.us

www.osc.state.ny.us **October 2010**

Table of Contents

The Practice of Internal Controls

The purpose of this management guide is to provide practical information about internal controls for local government financial operations. The control procedures discussed in this guide are presented in an easy reference format which lists individual controls (for specific financial areas) and the reasons why the control is important. Choosing the right internal controls and ensuring that they are consistently applied will help ensure that local governments are using public assets efficiently and protecting against loss, waste and abuse.

Information technology (IT) will most likely affect all or many aspects of local government financial operations and should not be considered a separate and distinct area of internal control. IT internal controls permeate many aspects of financial operations and should be reviewed in conjunction with each department or functional area of responsibility. Section 9 contains information on IT internal controls that will be of value to many local governments, especially those which do not employ IT specialists.

This manual is not meant to be a replacement or a substitute for locally developed internal control manuals. Rather, this guide should be used as a resource to improve the design of existing internal controls and to design new procedures required by changes in your operating and financial environment. Optimally, your control procedures should be described in a written internal control manual. Copies of your manual should be distributed to all managers and department heads who are responsible for implementing and supervising the application of your control procedures.

This guide contains examples of internal controls in the following financial areas:

Section 1 - Cash Receipts

Section 2 - Cash Disbursements

Section 3 - Bank Accounts and Bank Reconciliation Procedures

Section 4 - Billed Receivables - User Charges

Section 5 - Procurement

Section 6 - Payroll

Section 7 - Distinguishing Employees From Independent Contractors

Section 8 - Equipment and Consumables

Section 9 - Information Technology

Section 10 - Outsourced Services

In addition to this guide, we have also published a second internal control guide entitled *Management's Responsibility for Internal Controls*.[1] This companion guide discusses the theoretical aspects of an internal control framework and explains how this framework fosters an effective system of internal controls. Governing boards, as well as other local government officers and managers, will benefit from understanding both the practical and the theoretical aspects of a system of internal controls.

[1] **http://www.osc.state.ny.us/localgov/pubs/lgmg/managementsresponsibility.pdf.**

Identifying Risks

Each local government has its own unique set of circumstances and risks that will affect the design and implementation of its controls. Before determining which controls should be implemented, officers should assess the risk of fraud or errors occurring and remaining undetected. For example, is there a risk that:

- Wire transfers could be executed without management's knowledge?
- Purchases could be made for improper purposes?
- Accounting errors will not be detected?
- Cash receipts could be stolen without detection?
- Unnecessary or unauthorized overtime will be incurred?
- The lack of passwords will allow access to personal or confidential information?

After identifying risks, officers can begin to design a set of internal controls to mitigate or reduce those risks. The design process should consider the relationship between the cost of implementing the control and the benefits to be gained. When it is not practical or not cost-effective to implement certain controls, and the control is not otherwise required by law, supervisory review of work performed should be considered as a way to mitigate risk.

Monitoring

Identifying risks and implementing control procedures will not protect assets and produce reliable financial information if employees are not following established procedures. To ensure that controls are effective, department heads and supervisors should regularly review available documentation and accounting records to confirm that controls are being executed as designed. It is also important to consider the feedback received from employees. Some control procedures may appear to be a good solution to an identified risk but, once implemented, may cause unforeseen problems or inefficiencies. Other activities may not appear to need controls, yet upon further analysis, some type of control may be warranted.

Segregation of Incompatible Duties

Segregation of incompatible duties is a commonly used and widely accepted internal control practice.[2] Implemented effectively, this control reduces the risk that any employees will be able to carry out and conceal errors or fraud in the normal course of their duties without being detected. In general, there are three categories of duties or responsibilities that are examined when segregation of duties is discussed:

- Custody of assets
- Authorization or approval of transactions affecting those assets
- Recording or reporting of related transactions.

Ideally employees performing any one of the above functions would not also have responsibilities in either of the other two functions. The objective of segregation of duties is to prevent one person from having access to assets and responsibility for maintaining the accountability or authorizing transactions affecting those assets. The level of risk present should also be considered when developing a plan to segregate incompatible duties. When a high level of risk is present (e.g., when dealing with negotiable assets such as cash, negotiable checks, and inventories), there is a greater need for proper segregation of duties.

When it is neither practical nor cost-effective to segregate the basic responsibilities discussed above, compensating controls should be considered. Compensating controls are supervisory or other oversight procedures designed to reduce the risk of errors or fraud not being detected. Compensating controls frequently provide for regular review of work performed by individuals who have custody of assets and who also approve or record transactions affecting those assets. For example, when a local government's central treasury function is handled by one or two individuals, it is unlikely that incompatible duties can be adequately segregated. In these situations, a governing board member (or an internal auditor) should be designated to review accounting records, bank statements, check images and financial reports on a regular basis to ensure that fraud or significant errors are not occurring and remaining undetected. Most small local governments will need to consider compensating controls because financial duties are usually concentrated in one or two individuals.

The Office of the State Comptroller is available to assist you with any questions you may have about the internal controls discussed in this guide. A listing of regional offices and their telephone numbers is located at the end of this publication.

[2] Note that, in some instances, as a matter of law, local government positions are incompatible. In those cases, it is illegal for one person to simultaneously hold both positions. You should consult with the attorney for your local government if you have questions on whether the holding of two or more particular positions by the same person is incompatible and, therefore, illegal. The discussion here presumes that the individual performing the incompatible functions is doing so while holding a single position, or is holding two or more separate positions that are not incompatible as a matter of law.

Cash Receipts

Before officers can select and implement controls suitable for the size and complexity of their operations, they must first understand how, when, and where cash is collected and the duties performed by each employee. Although no system is foolproof, a well-designed set of control procedures can provide reasonable assurance that significant thefts of cash receipts and significant record-keeping errors will be prevented or detected. Cash, above all other local government assets, has the greatest potential for theft if a system of internal controls is not in place and functioning effectively.

This section outlines controls for reducing the risk of theft or errors during the collection, recording, and depositing of cash receipts. Procedures in this section may also apply to the collection of billed user charges and departmental operations that include the collection of cash receipts.

In this section the term "cash" refers to money, checks and money orders.

Collection Procedures

1-1-1 Centralize cash collections within a department or for the local government as a whole, when possible.

Reason for Control

Fewer locations and fewer employees collecting cash reduces opportunities for theft to occur and provides better accountability over cash collections. To the extent practical and consistent with law, the cash collection function should be centralized in the office of the chief fiscal officer or treasurer.

Note: Certain officers, such as County Clerks, County Sheriffs, Town Clerks, and Tax Collectors are required by law to collect cash receipts pertaining to their offices and generally to remit their collections to the chief fiscal officer or other parties periodically. The controls that follow can be applied to these operations also.

1-1-2 Assign a separate cash drawer to each employee responsible for collecting cash.

Reason for Control

Assigning a separate cash drawer to each collector provides individual accountability over the cash received by that person. If an employee is stealing, separate cash drawers and individual accountability will make it easier to trace the theft to the responsible party.

1-1-3 Restrictively endorse checks as soon as they are received.

Reason for Control

Immediately limiting the negotiability of checks ensures that checks received can only be deposited into a local government's bank account.

1-1-4 Instruct collectors that personal or payroll checks cannot be cashed from moneys in their cash drawers.

Reason for Control

This policy makes it clear that employees may not temporarily "borrow" cash and cover the removal with a personal check, even if temporarily. It also reduces the risk of noncollection on bad employee checks.

1-1-5 Instruct collectors not to accept checks for amounts over the amount due.

Reason for Control

Local governments are not banks and providing "cash back" services to customers should not be allowed.

1-1-6 Where no other evidence satisfactory for the purpose of audit is available, a serially press-numbered duplicate receipt form should be issued for any cash, checks, or money orders received. One copy should be provided to the customer and one copy should be retained for audit purposes.[3]

Reason for Control

Duplicate receipt forms provide an audit trail for moneys received when the amounts collected cannot be confirmed by other records, such as tax bills or billing stubs and remittance advices.

1-1-7 The office copy of issued receipt forms should be periodically reviewed by supervisory personnel, and any gaps or missing receipt forms should be investigated. Both copies of voided receipts should also be retained.

Reason for Control

A missing receipt form may indicate that a transaction has not been recorded or funds have been stolen and the receipt destroyed to hide the theft. A pattern of missing receipts is a red flag that should be investigated.

1-1-8 At locations or departments that collect fines or fees, such as a justice court or a solid waste facility, post a sign that states, "Please call xxx-xxx-xxxx if you don't receive a receipt."

Reason for Control

Involving the customer in ensuring they receive a receipt for miscellaneous fees and charges (not evidenced on a tax bill or other billing notice) reduces the risk that the employee collecting the cash may not record all receipts or record the receipt for a lesser amount.

[3] A requirement for receipts is set forth in statute. General Municipal Law Section 99-b requires every officer or employee who receives payment of money for or on behalf of a local government to issue a receipt to the person paying, when no other evidence satisfactory for the purpose of audit is available. The statute also requires that the officer or employee retain a copy of the receipt. The receipt and copy must be numbered consecutively.

Deposit Procedures

1-2-1 Secure undeposited cash and prepared deposits in a vault or safe (or other locked storage) until they are deposited in the bank. Restrict access to the vault or safe, or keep other storage methods locked when not in use.

Reason for Control

Securing cash limits unauthorized access before it can be deposited in the bank.

1-2-2 Deposit cash timely.

Reason for Control

Certain local government officers are required by law to deposit within certain timeframes. Consult with your local government attorney for guidance on laws specific to your office. However, while the statutory deadline is the latest point in time at which a deposit may be made, from an internal control perspective, the best approach is to deposit moneys as soon as possible. The longer money remains undeposited, the greater the risk that loss or theft can occur.

1-2-3 Deposit cash receipts intact.

Reason for the Control

"Intact" means that all cash collected since the last deposit must be deposited in the same form as it was collected (cash, check, or money order). This practice deters the cashing of checks from the proceeds of collections.

1-2-4 Prepare and maintain detailed deposit slips. Deposit slips must be detailed enough to identify the composition of the deposit between cash collected and individual checks deposited.

Reason for Control

Cash receipt transactions can be easily identified, traced, and corrected if detailed deposit slips are prepared.

1-2-5 The person who performs the bank reconciliation should be the final custodian of all deposit slips.

Reason for Control

Any discrepancies identified during bank reconciliations may be resolved by comparing the activity in the bank and accounting records to deposit slips.

1-2-6 The governing board should establish a charge for checks returned for non-sufficient funds (NSF).[4] Notification of the NSF check charge should be included on all billings and posted in public view.

Reason for Control

An NSF charge will deter customers from issuing checks that will not clear the bank and it will also help cover time spent by employees recouping NSF check funds.

Record-Keeping Procedures

1-3-1 Record receipts in the accounting system timely.

Reason for Control

Accountability over cash receipts is enhanced when cash is recorded in the accounting records as soon as practicable from the date cash is received. The longer receipts go without being entered into the accounting system, the greater the risk an employee could misappropriate funds.

1-3-2 For each cash drawer, daily cash collection records or cash register tapes should be reconciled to the amount of cash on hand at the end of the day (sometimes referred to as the daily "cash-out").

Reason for Control

Daily cash-out procedures help to uncover discrepancies between actual cash collected and recorded amounts in a timely manner.

1-3-3 Employees responsible for collecting cash and preparing bank deposits should not record cash transactions in the accounting records.

Reason for Control

The basic rule in play here is the need to segregate asset custody from record-keeping duties. Segregating the duties of "receiving cash" from "recording cash transactions" prevents a single employee from stealing undeposited cash (or substituting checks received for cash taken) and altering cash receipt journals or other records to disguise the theft. Similarly, segregating the duties of preparing or making bank deposits from recording duties prevents an employee from removing cash from a bank deposit and altering accounting records to disguise the theft.

[4] General Municipal Law Section 85 sets forth the authority of governing boards of municipal corporations to impose a service charge to any account owing to the municipal corporation where a check tendered as payment was dishonored by a bank or other depository institution. The statute indicates the maximum amount that may be charged and how the service charge is collected.

Cash Disbursements

Local governments make a wide variety of cash disbursements, mostly by check, but to a lesser degree by wire transfer for bond and note payments; by direct deposit for net payroll amounts when properly authorized; and, in cash, for petty cash disbursements. Contrary to common assumptions, fraud actually occurs more frequently in the cash disbursement cycle than in the cash receipt cycle. Advances in online banking and other digital technologies have made the cash disbursement cycle even more susceptible to fraud by perpetrators from outside the local government.

This section discusses internal controls that will reduce the risk of theft or loss occurring during the preparation, authorization and distribution of checks. This section also covers controls related to banking, petty cash, and wire transfers.

Check Preparation Procedures

2-1-1 Assign an employee not responsible for check preparation to order checks, inventory them, and to identify reasons for gaps in the numbering sequence. Issue pre-numbered checks in sequence.

Reason for Control

Assigning responsibility for ordering and inventorying pre-numbered check stock reduces the risk that blank checks will be lost or misused without detection. Pre-numbering establishes an audit trail over check disbursements.

2-1-2 Keep blank checks and check stock secure at all times.

Reason for Control

Securing blank checks and check stock in a locked environment helps prevent their misuse.

2-1-3 Make checks payable to a specific payee or custodian - never to "cash" or "petty cash."

Reason for Control

Making checks payable to a specific payee reduces the risk that someone could fraudulently cash a check not intended for them.

2-1-4 If financial software is used to print checks, restrict the use of hand-drawn checks.

Reason for Control

Frequently, application controls are built into computerized financial modules to detect or prevent payments to unauthorized payees or the disbursement of suspicious dollar amounts. IT application controls can be circumvented by issuing hand-drawn checks; hence their usage should be controlled and limited.

Check Signing Procedures

2-2-1 The official responsible for check preparation and signing should not have the authority to solely (or individually) audit and approve claims for payment.

Reason for Control

Segregating check preparation and check signing from the audit and approval of claims prevents an official (or employees under his or her control) from making improper purchases, approving them for payment, and then preparing the check to pay for such purchases without being detected.

2-2-2 Limit check signing authority to as few officers as possible and only to those positions authorized by law to sign checks.

Reason for Control

Limiting check signing authority reduces the opportunity for fraudulent checks to be written and signed. Each locality should consult with its attorney regarding statutory authorizations for signing checks.

2-2-3 The official responsible for signing checks (or a deputy) should compare prepared checks to an audited and approved warrant or a payroll register prior to releasing such checks.

Reason for Control

Comparing prepared vendor checks to the listing of audited and approved claims and comparing prepared net payroll checks to the payroll register can assist in the detection of unauthorized or erroneous checks before they are sent to vendors or distributed to employees.

2-2-4 Electronic signature disks or other forms of facsimile signatures should be secured in a locked location under the control of the signatory. Signature disks or other facsimile signatures should only be used under the direct supervision of the official (or deputy) whose signature is on the disk.

Reason for Control

The official responsible for signing checks should always ensure that any facsimile of his or her signature is protected from unauthorized use. To prevent unauthorized use of facsimile signatures, the official with signatory authority (or his or her deputy) should be present whenever his or her signature is applied to prepared checks.

2-2-5 Do not sign blank checks.

Reason for Control

A blank, signed check may be used for any purpose and for any amount. Signing a blank check increases the possibility that a check could be made payable to an unauthorized payee or for an unauthorized amount.

2-2-6 After checks are printed, someone outside the check processing function should account for all checks printed, voided or returned to stock unsed.

Reason for Control

Accounting for all checks helps ensure that no checks are lost, stolen or misused.

Petty Cash Procedures

2-3-1 A petty cash fund must be established (increased or decreased) only in accordance with legal requirements, generally, by resolution of the governing board. The resolution should establish the custodian and amount for the fund. Petty cash funds should be authorized at the lowest amount practical.

Reason for Control

Board authorization establishes accountability over the amount authorized for petty cash and designates the person responsible for safeguarding and maintaining petty cash records.

2-3-2 Custody of the petty cash fund should be assigned to only one employee. As petty cash custodian, this employee should handle all petty cash transactions and should secure the fund in a locked location separate from other cash drawers.

Reason for Control

Having more than one person with access to the petty cash fund diminishes the accountability and security of this fund. Restricting access to the petty cash fund is the best way to prevent unauthorized use or theft of petty cash.

2-3-3 A voucher (or claim) requesting reimbursement of petty cash expenses should be submitted to the claims auditing body or claims auditing official, consistent with law. Original receipts for all petty cash expenditures should be attached to the voucher.

Reason for Control

The examination of petty cash expenditures by the claims auditing body or claims auditing official deters improper petty cash expenditures and ensures that requests for reimbursement are appropriate. Original receipts provide proof of what was purchased and are the basis for replenishing the fund.

2-3-4 The custodian of the petty cash fund should periodically reconcile petty cash on-hand and unreimbursed receipts to the petty cash amount authorized by the governing board.

Reason for Control

Periodic reconciliations ensure that all petty cash is accounted for.

Wire Transfer Procedures

2-4-1 All wire transfers should be made at the direction of the chief fiscal officer or other officer having custody of the monies being disbursed, or in their absence, by their deputies. Before approval is granted, documentation detailing the amount, purpose, and destination of the wire should be presented for review. Such documentation should be retained for audit purposes.

Reason for Control

Preapproval of wire transfer documentation will reduce the occurrence of errors or fraud occurring in electronic transfers. Generally, wire transfers cannot be easily retrieved, if at all, so it is important that all wire information be 100 percent accurate.[5]

2-4-2 If wire transfer software resides on a local hard drive, secure the computer on which the software resides in a locked room if possible and with password protection.

Reason for Control

Restricting access to computers with wire transfer capability reduces opportunities for unauthorized individuals to execute wire transfers.

2-4-3 If using in-house wire transfer software, the chief fiscal officer or other authorized officer, and the IT department should be knowledgeable about application controls available in the software. Such application controls should be activated at the levels appropriate for the scope of wire transfer activity.

Reason for Control

Application controls, such as limit controls, can be set to prevent the execution of wire transfers unless certain pre-established conditions are met.

2-4-4 If using in-house wire transfer software, consider requiring two passwords to be provided before a wire transfer can be executed.

Reason for Control

Dual passwords (executed by different individuals) will prevent the person preparing the wire transfer from transmitting it without supervisory approval.

[5] General Municipal Law Section 5-a provides that, whenever an officer of a local government is authorized or directed to disburse or transfer funds in his or her custody, the officer may do so by means of an electronic or wire transfer. All such disbursements are subject to laws that are otherwise applicable to disbursements or transfers (e.g., audit of claims requirements) and the governing board of the local government must have entered into a written agreement with the depository bank or trust company containing certain terms and conditions as set forth in section 5-a. The statute requires that the bank or trust company provide to the officer ordering the transfer written confirmation of each transaction no later than the business day following the day on which the funds are transmitted. It further makes it a duty of the governing board to adopt a system of internal controls for the documentation and reporting of all wire or electronic transfers.

2-4-5 If using in-house wire transfer software, ensure that firewalls and intrusion detection capabilities are installed and working properly.

Reason for Control

It is important to protect wire transfer computers from external intrusions by hackers.

2-4-6 If initiating wire transfers by telephone or fax, require the transmitting bank to confirm the amount and destination of the transfer by calling a supervisor or another employee before the wire is executed.

Reason for Control

By requiring the bank to confirm telephone or fax requests, the opportunity for a single employee to execute an improper or inaccurate wire transfer will be controlled.

2-4-7 Employees who execute wire transfers should not prepare or post journal entries or reconcile bank accounts. When it is not practical to segregate these duties, a compensating control, such as supervisory review of journal entries, should be considered.

Reason for Control

Segregating the execution of wire transfers from the recording and reconciliation functions prevents a single employee from controlling the execution, accounting, and reconciliation of wire transfer activity and thereby limits the opportunity for disguising a wire transfer error or fraud.

Bank Accounts and Bank Reconciliation Procedures

Safeguarding bank account information has become increasingly important in today's electronic environment. Access to bank account information creates an opportunity for fraudsters to create phony checks and fictitious wire transfers from computers anywhere in the world. All bank account information and bank passwords should be safeguarded both within and outside the organization. Requests for bank account information originating from outside the local government should be verified before any information is provided. Only known and authorized personnel should be given access to bank account information. Ensuring that bank reconciliations are prepared timely is also an effective internal control for detecting accounting and banking errors and for identifying fraudulent transactions originating from outside the local government.

This section discusses practical and cost-effective internal controls that can be used to protect banking information.

Bank Account Procedures

3-1-1 Inform all depositories in writing that only the chief fiscal officer (or other officers having custody of monies and authorized to have a bank account) or their deputies, are permitted to open or close bank accounts for general governmental purposes.

Reason for Control

Providing clear direction to depositories regarding the authority to open and close bank accounts prevents officers and employees from establishing unauthorized or secret bank accounts in the name of the local government.

Note: In addition to chief fiscal officers, certain officers such as a county sheriff, county clerk, town and village justices, and town clerks, have authority to open bank accounts for their departmental operations.

3-1-2 Keep your federal tax ID number in a secure location not available to other officers, employees, or to the public.

Reason for Control

A federal tax ID number can be used (in lieu of a Social Security number) to open a bank account.

3-1-3 The chief fiscal, other authorized officer, or internal auditor should periodically ask each depository for a listing of all bank accounts in the name of the local government and for all bank accounts carrying the local government's federal tax ID.

Reason for Control

A periodic review of the bank accounts listed in the name of your local government or associated with your federal tax ID is a good way to detect accounts that may have been opened without the knowledge of the chief fiscal officer or other officer. This type of review also detects nongovernment accounts opened with the local government's federal tax ID number.

3-1-4 When an official authorized to sign checks or to perform wire transfers leaves the local government, immediately contact the bank and revoke his or her check signing authority, online banking capabilities and wire transfer authority, and destroy his or her signature disk.

Reason for Control

Revoking signatory authority and other banking privileges ensures that ex-officers or ex-employees cannot make unauthorized banking transactions after they leave local government employment.

Bank Reconciliation Procedures

3-2-1 Bank reconciliations should be prepared monthly and any differences between net bank balances[6] and general ledger cash accounts should be researched and explained. A supervisor should review the monthly bank reconciliation and authorize any correcting entries needed.

Reason for Control

Bank-to-book reconciliations assist in the detection of record-keeping errors and fraud. Supervisory review of bank reconciliations also ensures the timeliness of bank reconciliations and the authorization of any corrections necessary. A sample bank reconciliation is included in Appendix A.

3-2-2 Bank reconciliations should be performed by an employee or official who does not have custody or access to cash and who does not record cash receipt, cash disbursement, or journal entry transactions.

Reason for Control

Segregating the incompatible duties of custody of cash, record-keeping, authorizations, and reconciliations prevents an employee or official from controlling all phases of the accounting function. When one person controls all phases of the accounting function, the opportunity for errors and fraud to go undetected is high.

[6] A net bank balance is determined by adding deposits in transit and subtracting outstanding checks (and other pending charges) from the gross bank balance as of a certain date.

Bank reconciliations should be performed by an employee who does not have custody of or access to bank accounts or cash and who does not authorize, record, or adjust cash receipt or cash disbursement transactions. In small, one-person offices, where it is not possible to segregate these duties, accounting entries and bank reconciliations should be reviewed monthly by a supervisor. In the smallest of local governments, a designated member of the governing board may need to serve in a supervisory role over the accounting function. Supervisory (or board) oversight acts as a compensating or mitigating control to the inadequate segregation of accounting duties. An employee who controls all phases of the accounting function can potentially disguise a theft of cash or the issuance of a fraudulent check by altering accounting entries or preparing fictitious bank reconciliations.

3-2-3 During the bank reconciliation process, check images (or cancelled checks) and bank statements should be reviewed for anything out of the ordinary, such as suspicious payees, large dollar amounts, and secondary endorsements. All check images should be retained in electronic format for audit purposes.

Reason for Control

Reviewing check images and bank statements can identify suspicious or erroneous transactions.

3-2-4 Keep bank statements and check images in a secure location.

Reason for Control

In today's digital environment, forged checks are easier than ever to produce. Protecting your bank account numbers will help lower the possibility of forged checks occurring.

3-2-5 Shred all banking correspondence not required to be maintained to prevent duplication of checks and to limit access to bank account information.

Reason for Control

Banking correspondence (including bank statements and check images) must be maintained for the period of time specified in the appropriate records retention schedule. Local governments may obtain a copy of their Records and Retention Schedule at http://www.archives.nysed.gov/a/records/mr_pub_mu1.shtml. School districts may obtain a copy of their schedule at http://www.archives.nysed.gov/a/records/mr_pub_ed1.shtml.

Billed Receivables - User Charges

Local governments often provide water, sewer, and even electric services for their residents and other user customers. Properly designed accounting records and reports should be in place to ensure that total billings and individual customer accounts are accurately accounted for, collections are recorded timely, and delinquent accounts are readily identified and enforced. Periodic reconciliations of control accounts to individual customer accounts are also important to ensure the overall accuracy of the accounting records. All of these controls will help promote accountability and collectability of billed user charges.

Most user charges are processed electronically on applications (software) that have been developed in-house or purchased from an outside vendor. In addition to the billing, collection, and reconciliation controls discussed below, appropriately designed IT general controls should also be put into place and monitored for effectiveness. Each software package may also have application controls built into it that may assist management in implementing controls over billed receivables.

This section discusses procedures that should be in place to ensure that user charges are properly accounted for and delinquent accounts are enforced. Section 1 of this guide discusses internal controls over cash receipts that are also germane to the collection of billed receivables.

Policy Guidance

4-1-1 The governing board should create a written policy establishing, consistent with legal requirements, the frequency of user charge billings; billing rates; collection periods; the timing and amount of late charges; the enforcement of unpaid accounts; and any other guidelines necessary for the effective financial management of the service provided.

Reason for Control

Officers and employees need guidance on how to administer user charges and the financial aspects of providing these services. By establishing financial guidelines in a written policy the board will enable officers and employees to understand its expectations regarding billing, collection, and enforcement processes for user charges.

Properly Designed Records

4-2-1 Individual customer accounts should include sufficient information to identify the names of the individuals responsible for payment of the bill, location of the property, mailing address (if different), account number, usage (actual or estimated), billing rates, and amount billed. A unique customer account code should be established for each account.

Reason for Control

Customer accounts provide a record of past billings and consumptions, collections, adjustments (if any), and unpaid balances for each customer.

4-2-2 Electronic (as well as manual) billing records or reports should include the grand total billed to all customers for the period.

Reason for Control

Billing grand total information is essential to establish accountability for amounts to be collected and helps serve as the basis for posting entries to receivable control accounts, such as, SW380, the water rents receivable general ledger account.

4-2-3 Bills should include an identifying section to be returned with the payment. The identifying section should include the name, address, account number, and method of payment (cash, check, money order).

Reason for Control

The identifying (return) section of the bill helps ensure that the correct property owner or customer account is credited, and also provides evidence of payment for audit purposes.

4-2-4 The face of each bill should instruct customers to communicate complaints about billing and other record-keeping errors directly to supervisory personnel.

Reason for Control

Patterns of customer complaints may indicate systemic errors in the billing and collection process or may be a red flag for possible fraud. Bringing these complaints to the direct attention of supervisory personnel allows supervisors to evaluate the legitimacy and impact of the complaints and authorize corrective action when necessary.

Billing and Adjustment Procedures

4-3-1 In a small municipality with few people involved in the financial operations, the total amount to be billed for each period should be recorded in the minutes of the board's proceedings.

Reason for Control

Recording (in the minutes) the total amount billed not only informs the governing board of amounts expected to be collected, but also provides the basis for establishing accountability to those charged with collecting and reconciling amounts billed. It also helps prevent unauthorized changes to billing totals from occurring after bills are sent out.

4-3-2 The governing board or other authorized supervisory personnel should approve all billing adjustments, write-offs and refunds prior to such adjustments or refunds being made. The reasons for all adjustments should be documented and retained for audit purposes.

Reason for Control

Appropriate prior approval ensures that adjustments, write-offs, and refunds are made consistently and according to the locality's policy. In addition, requiring board or supervisory approval will reduce the opportunities for unauthorized adjustments, such as fake refunds to cover the theft of cash or reductions in billings to cover the nonpayment of an employee's personal bill.

Record-Keeping Procedures

4-4-1 Establish a separate receivable control account for each type of billed receivable (for example for water rents or sewer rents) to account for transactions related to the billed receivable process.

Reason for Control

A receivable control account is an accounting record for recording and summarizing total billings, total collections, adjustments, and the outstanding balance of billed receivables. A properly maintained receivable control account allows for the balance of billed receivables to be readily determined and reconciled to individual customer accounts.

Note: In those limited situations where a general ledger system is not in use, a receivable control account record for billed receivables should still be established and maintained as a stand-alone manual record.

4-4-2 Post payments received to individual customer accounts as soon as possible.

Reason for Control

Prompt recording ensures the accuracy of customer accounts.

4-4-3 Reconcile the receivable control account balance to the sum of individual customer account balances, preferably each month. Identify and resolve the cause of any differences between the control account balance and the sum of customer account balances.

Reason for Control

The reconciliation of the control account balance to the sum of the individual customer accounts is a valuable check on the accuracy of the accounting records. A difference between these two records may indicate that record-keeping errors or fraud may have occurred. Differences should be promptly pursued, resolved and records adjusted accordingly. Reconciliations provide little internal control if differences noted during the reconciliation process remain unresolved.

4-4-4 The reconciliation of the receivable control account balance to the sum of the individual customer accounts should be performed by someone independent of the cash collection and deposit duties.[7]

Reason for Control

Reconciliation of the detailed records to the control account is a key internal control in detecting record-keeping errors and patterns indicative of fraud. The reconciliation process should be performed by someone who is independent of the cash collection/deposit process and the recording of payments from customers.

[7] If these duties cannot be segregated, a designated board member or supervisor should review the accuracy and completeness of control account reconciliations to the listing of unpaid accounts.

Overdue/Delinquent Account Procedures

4-5-1 Apply interest and penalties in overdue customer accounts according to law and governing board policy, and record total interest and penalties in the receivable control account.

Reason for Control

Interest and penalties serve to encourage prompt payment and help pay for the administrative costs of the delinquent collection process. Applying interest and penalties uniformly ensures that no property owner or customer is granted a special favor.

4-5-2 Enforce delinquent accounts on a timely basis. A listing of delinquent accounts and the amounts due (base + interest and penalties) should generally be prepared and submitted to the board for approval at least once a year.

Reason for Control

Board review and approval of delinquent accounts provides an independent evaluation of the accounts and amounts deemed delinquent and also initiates the delinquent enforcement process.

4-5-3 In certain cases, delinquent receivables may be levied on the next real property tax roll. For example, a village's unpaid water charges may be added to the annual village tax levy of the property associated with the account in default.

Reason for Control

Enforcement of delinquencies by levy increases the chances that delinquent billed receivables will be collected when the next property tax bill is paid.

4-5-4 The accuracy and completeness of delinquent lists prepared for levy or other enforcement actions should be verified by someone in a supervisory or oversight role.

Reason for Control

Employees with billing or collection duties (or both) can disguise errors and fraud by omitting, adjusting, or listing fictitious delinquent amounts.

Analytical Procedures

4-6-1 Before bills are printed and sent to customers, a "reasonableness" check should be performed to assess the completeness and accuracy of the billing register and bills. The reasonableness check could include, for example, comparing the total amount to be billed with prior billing amounts, comparing current consumption with amounts billed, or comparing the number of bills to be printed with the database of user or customer accounts.

Reason for Control

Performing "reasonableness" checks will help identify potential billing problems before bills are mailed to customers. It is much easier to correct obvious errors before bills are generated and sent than after that time.

4-6-2 Periodic comparisons between volume of services delivered (such as water, electric, or gas) should be made to the total volume billed. After taking into account industry benchmarks for waste or loss, significant differences between volume delivered and volume billed should be investigated.

Reason for Control

Significant differences between volume delivered and volume billed may indicate unauthorized or unknown uses of services that are not being billed. It may also indicate a need for infrastructure repairs or new meters to reduce volume being lost or not recorded.

Procurement

Having appropriately designed controls in place for procurement not only protects against the misuse of taxpayer dollars, but also enhances employee awareness and attitudes toward controlling the cost of essential purchases. The larger the organization and the more decentralized the procurement function is, the greater the importance of control procedures over purchasing. Each locality must design a system of procurement controls that are appropriate for the size, locations, and structure of its operations. Internal controls over procurement should be designed to ensure that unauthorized purchases are prevented; cost considerations are evaluated; nonessential purchases do not occur; and statutory requirements are followed to ensure fair and open competition, and cost- effectiveness in the purchasing process.

This section discusses internal controls designed to ensure the efficiency and cost- effectiveness of the procurement process. Controls over the preparation and signing of checks are covered in Section 2 of this guide, "Cash Disbursements."

Procurement Procedures

5-1-1 Clear lines of authority for approving purchases (before they occur) should be established. Depending on the size of the local government, approvals may consist of verbal approvals or, in larger local governments, requisitions or purchase orders (either electronic or manual) may be used to formally document the request and approval process.

Reason for Control

Purchase approvals, whether oral or written, help ensure that each purchase is necessary for local government operations and that cost considerations have been evaluated. Written approvals are superior, but cost considerations may necessitate oral approvals in smaller units of local government.

5-1-2 Prior to authorizing a major purchase and periodically for routine purchases, the availability of budget appropriations should be verified. In an electronic system, application controls should be built into the software to prevent the approval of a requisition or the issuance of a purchase order if sufficient appropriations are not available. In other systems, the budget officer should be consulted to determine the availability of appropriations.

Reason for Control

Checking the availability of appropriations will ensure that authorized purchases do not exceed budget authorizations.

5-1-3 Where practical, the approval to purchase goods or services should be authorized by personnel other than the employee requesting the purchase; the approval to purchase should also be segregated from the receiving of goods and services.

Reason for Control

By segregating the approval to purchase from the request to purchase and the receiving of assets or services purchased, the opportunity to make personal purchases from public funds (and for these transactions to remain undetected) is reduced.

Properly Designed Forms and Record-Keeping Procedures

5-2-1 All purchasing forms (such as requisitions and purchase orders) should be designed to include specific details about the items or services to be purchased including quantity, costs, model numbers, terms of sale, availability of appropriations, and approvals to purchase.

Reason for Control

Properly designed forms allow comparisons to be made between items requested and items purchased in terms of descriptions, quantities, and prices. Forms are also used to record the approval to purchase and thereby limit unauthorized purchases from occurring. Properly designed forms provide an audit trail on the purchasing process from start to finish.

5-2-2 All purchasing forms should be sequentially numbered.

Reason for Control

Sequential numbering allows for the tracking of issued requisitions and purchase orders and for the cancellation of unused purchase orders.

5-2-3 Purchasing forms should have multiple copies so that other departments such as receiving and accounts payable can be notified of the authorization to purchase goods and services.

Reason for Control

Multiple copies facilitate communication (especially in large local governments) about the ordering and expected arrival dates of items or services purchased.

5-2-4 Access to the module for creating new vendors should be segregated from employees who authorize purchases or approve claims for payment.

Reason for Control

In a computerized purchasing environment, segregating the duties of creating new vendor accounts from the duties of authorizing purchases and approving claims for payment lessens the opportunity for establishing fictitious vendors and making payments to them.

5-2-5 Complete street addresses and Social Security numbers (or federal tax ID numbers) should be obtained for all vendors and entered into the vendor master file.

Reason for Control

Post office boxes can be used to disguise phony vendor operations. For the purposes of issuing 1099s and to discourage the creation of fictitious vendors, Social Security or federal tax ID numbers should be required before new vendors are added to the master file.

Note: Federal tax ID numbers and Social Security numbers generally are confidential and, as such, access to them should be properly safeguarded and restricted to only those employees who need this information to perform their duties.

5-2-6 Once goods or services have been approved for purchase, appropriations can be reserved for the estimated amount of the approved purchase or service by establishing an encumbrance. Encumbrance accounting is most efficient when the requisition or purchase order process is computerized and an encumbrance is established automatically when a purchase order is issued. For smaller local governments without sophisticated computerized purchasing systems, encumbrances for high cost purchases and services should be recorded via journal entry.

Reason for Control

Encumbrance accounting provides budgetary control over purchases and services. When an encumbrance system is in place, it will help prevent budgetary line items from becoming overexpended.

5-2-7 Before the close of the fiscal year, the finance department should review all outstanding encumbrances and determine if amounts designated should be continued, adjusted, or cancelled.

Reason for Control

Sometimes goods or services are ordered and never received, but the original encumbrance isn't liquidated. In other instances, encumbrances are established "in bulk" at the beginning of the year but are not completely utilized. To ensure proper financial reporting, outdated and nonspecific encumbrances should be liquidated before the end of the fiscal year.

Receiving Procedures

5-3-1 When goods or services are delivered, receiving or packaging slips should be verified against the quantity, type, and condition of the goods received. Amounts received should also be compared to amounts ordered, as described on the purchase requisition or purchase order. Verified receiving slips should be forwarded to the person responsible for preparing the claim voucher.

Reason for Control

Verification of the accuracy of receiving slips to both the actual goods received and to the requisition or purchase order will usually detect shipping errors and ensure that payment will only be made for quantities ordered and received in satisfactory condition.

5-3-2 The responsibility for the receipt and verification of items ordered should be segregated from the employee who requested or authorized the purchase.

Reason for Control

An employee with both of these responsibilities could order items that are not necessary and keep them for personal use without being detected.

Payment Procedures

5-4-1 Each department that ordered goods or services should assemble a voucher or claim package containing: the verified receiving slip, the approved purchase order (if applicable), the original invoice and the certification or signed approval of the department head stating that the goods or services were received and they are a true and just charge. All voucher packages should be forwarded to the claims auditing body or official, or other appropriate officer as provided by law.[8]

Reason for Control

The voucher package is the basis for the audit of claims. A properly prepared voucher package will help ensure that payments will only be authorized for goods and services actually received, that are of acceptable quality, and that further a lawful purpose of the local government. A complete voucher package also lessens the risk that unauthorized purchases and services will be paid for without detection. Payments to legitimate vendors may be delayed if a complete voucher package is not presented for the claims auditing body or official.

5-4-2 Even if not required by statute, goods should be received and/or services rendered before a voucher or claim is submitted.

Reason for Control

A requirement that goods and services are received before payment serves to ensure that purchases are legal and necessary for local government operations and were received or performed in a satisfactory manner. It also helps avoid to the potential for making a constitutional gift to a vendor who has already been paid, but ends up not providing the agreed upon goods or services.

5-4-3 Vendor checks should not be returned to the department or the official who requested or made the purchase. Checks should be mailed directly to vendors.

Reason for Control

Direct mailing of vendor checks prevents an employee from intercepting a check written to a phony vendor or for delaying payments to vendors to solicit gifts or other gratuities.

[8] Statutory requirements for presentation and auditing of claims vary, and you should with your local government's attorney if questions arise. For additional guidance on the claims auditing process, see our Local Government Management Guide entitled *Improving the Effectiveness of Your Claims Auditing Process* on the web at: **http://www.osc.state.ny.us/localgov/pubs/lgmg/claimsauditing.pdf.**

Statutory Controls[9]

5-5-1 With certain exceptions, purchases of goods in excess of $20,000 and contracts for public work (e.g., services) in excess of $35,000 must be acquired in accordance with competitive bidding requirements as provided for in General Municipal Law Section 103.

Reason for Control

One of the goals of competitive bidding requirements is to foster honest competition so that quality commodities and services are obtained at the lowest possible price. Competitive bidding also guards against favoritism, extravagance and fraud, while allowing interested vendors a fair and equal opportunity to compete.

5-5-2 Every local government must adopt its own policies and procedures for procurements of goods and services not required by law to be competitively bid. The law generally requires that the procurement policy provide that alternative proposals or quotations be obtained by use of written requests for proposals (RFPs), written or verbal quotations, or other methods, for procurements that are not subject to bidding requirements.

Reason for Control

Procurement policies and procedures generally ensure that competition is sought in a reasonable and cost-effective manner for procurements below the bidding thresholds and for other contracts exempt from bidding.

Analytical Review Procedures

5-6-1 Management or their designee should periodically review a listing of vendors and cumulative amounts purchased from individual vendors.

Reason for Control

Reviewing vendor listings provides management with a "big picture" of the scope and nature of all purchases made. The review may identify opportunities for cost savings and can be used to identify aggregate purchases that may be subject to competitive bidding. Unusual or unknown vendors may also be detected during this type of review.

[9] The $20,000 and $35,000 bidding thresholds became effective on June 22, 2010, and November 12, 2009, respectively. For additional information about procurements, see our Local Government Management Guide entitled *Seeking Competition in Procurement* available on the web at: **http://www.osc.state.ny.us/localgov/pubs/lgmg/seekingcompetition.pdf.**

Payroll

Payroll and related employee benefit costs are by far the largest component of nearly every local government budget. The establishment of strong internal controls over payroll ensures that employees are paid the correct salary and wages, and opportunities for payroll errors and fraud are controlled. Some examples of payroll frauds include ghost employees (someone receiving a paycheck who does not actually work for the local government); overstating regular or overtime hours worked; increasing rates of pay without board approval; and continuing employees on the payroll after termination. Internal controls also provide assurance that the large volume of information required for every payroll is processed quickly and accurately.

This section discusses internal controls designed to ensure the accuracy and the authenticity of payroll payments.

Authorization Procedures

6-1-1 The governing board, or such other body or officer as authorized by law, should establish and approve all salary and hourly wages by position or as part of a collective bargaining agreement. Subject to statutory requirements and collective bargaining agreement provisions, the board or officer should also establish the frequency of all payroll distributions (biweekly, monthly, etc).

Reason for Control

Establishing salaries and wages and the frequency of payroll periods is generally part of the board's oversight responsibilities. These authorizations prevent other officers or department heads from establishing new pay rates or schedules without proper approvals.

6-1-2 The terms and conditions of collective bargaining agreements should be clearly communicated to those responsible for payroll processing.

Reason for Control

Terms and conditions of employment that are not clearly articulated to those responsible for executing payroll activities can lead to uncertainty about payments and benefits and the overall rights, duties, and responsibilities of employers and employees. This uncertainty could further result in unnecessary costs and/or grievances or litigation for a local government.

6-1-3 If not otherwise segregated under the law, segregate payroll authorizations (hiring/firing, pay rate setting, and other payroll changes) from the preparation and processing of payroll records and checks. In a computerized payroll system, payroll changes should be entered into the system by the personnel department or an employee who does not process the payroll register and checks, if possible.

Reason for Control

Segregating payroll authorizations from preparation duties reduces the risk of a single employee establishing ghost employees, increasing hourly rates and salaries, or recording overtime not worked without being detected.

6-1-4 Limit access to computerized payroll applications and data files containing potentially confidential information such as social security numbers and deductions.

Reason for Control

The payroll process involves a range of confidential and personal information. Hence, access to computerized applications and paper files (such as personnel files) should be restricted to the fewest number of officers and employees possible.

Payroll Change Procedures

6-2-1 All changes in employment status (e.g., additions and terminations), salary, and wage rates should be properly authorized, approved, and documented to support employment status changes. When appropriate, payroll change forms should be used to document and authorize wage and salary changes authorized by the governing board.

Reason for Control

When a formal process exists to document authorized changes to salaries and wages, the opportunity for fraudulent or erroneous payroll changes to occur without detection decreases.

6-2-2 If payroll change forms are used, control access to these forms by keeping them in a locked cabinet or drawer.

Reason for Control

Limiting access to payroll change forms reduces the risk that fraudulent authorization could be made by forging authorized signatures and other information.

6-2-3 Prior written authorization should be required for all nonemergency overtime hours and should be granted only for specific, verifiable purposes, consistent with any collective bargaining agreements. In emergency situations, supervisors should verbally preapprove overtime to be incurred, and follow up with a review of overtime records to determine the appropriateness of overtime hours incurred.

Reason for Control

A simple way for hourly employees to perpetrate payroll fraud is to over-report overtime worked, particularly if supervisors are not on site during the overtime hours. Prior written or oral approval allows management to make sure that overtime is incurred for a valid and needed purpose, and that funding for the nonemergency overtime is provided for in the budget.

Time and Attendance Records

6-3-1 Require employees to document days and hours worked and leave credits used on either time sheets or time cards. Time sheets and time cards should be reviewed and approved by supervisory personnel who have direct contact with the employee.

Reason for Control

A lack of appropriate time and attendance records increases the likelihood that an employee could be paid for time not worked or for unauthorized absences.

6-3-2 Using time clocks to record arrival and departure times will provide additional control over days and hours worked by employees. Electronic time clocks can also reduce manual processing of payroll data if the time clock and payroll application are compatible.

Reason for Control

For local governments with large numbers of employees or where shift work is involved, an electronic time clock system will help ensure that employees are paid accurately for hours and days worked. An electronic time clock can also reduce data entry work if time clock entries can be downloaded directly into the payroll application.

6-3-3 Time clocks should be placed in an area where their use can be observed by supervisors.

Reason for Control

This will discourage employees from clocking in or out for co-workers who are not actually present.

6-3-4 Require the use of leave request forms to document advance requests to use accrued leave credits and to document absences covered by the use of leave credits.

Reason for Control

Leave request forms provide an audit trail on the use of accrued leave credits and assist with the preparation of accurate gross payroll amounts for individual employees.

6-3-4 Maintain leave accrual records and communicate leave balances to employees regularly.

Reason for Control

Maintaining and reviewing leave accrual records ensures that such records are accurate and that employees only receive payment for leave time they are entitled to.

Verification Procedures

6-4-1 Even if not otherwise required by law, before checks are distributed, payroll registers or similar records should be certified by the officer or employee having direct supervision over specific departments or individual employees. The certification should indicate that to the best of the supervisor's knowledge, services were actually performed by the persons listed on the payroll and that days and hours worked are accurate and justified.

Reason for Control

A review of the completed payroll register will help detect unusual or inaccurate payments requiring further verifications before checks are distributed.

6-4-2 Management or the internal auditor should periodically review payroll change reports. When unusual changes are identified, those items should be traced to authorization documents (i.e., board minutes, payroll change forms, or collective bargaining agreements).

Reason for Control

Managerial review of this type of report provides assurance that payroll changes are being properly authorized and input correctly.

Payroll Check Procedures

6-5-1 Payroll checks should not be distributed to employees prior to the actual pay dates.

Reason for Control

The premature distribution of paychecks to employees creates the possibility that a check will be deposited or cashed by an employee prior to the date it is legally valid.

6-5-2 Undelivered payroll checks should be returned directly to the chief fiscal officer or other authorized officer for safekeeping and eventual cancellation, if warranted.

Reason for Control

Like all checks, undelivered payroll checks are negotiable instruments and unauthorized persons may attempt to cash them if the opportunity presents itself. Undelivered payroll checks should not be returned to the person who processes payroll records or to the person who performs the payroll bank reconciliation.

6-5-3 Requests for direct deposit should be made in writing and kept on file for audit purposes.

Reason for Control

Direct deposits can be used to disguise payments to nonexistent employees.

6-5-4 In local governments with more than 100 employees, as part of the direct deposit program, periodically require employees to pick up their payroll statement in person.

Reason for Control

In large units of local government, a once-a-year verification of the legitimacy of all direct deposits may detect unauthorized or fictitious employees. It may also detect the continuation of terminated or retired employees on the payroll.

6-5-5 Pay checks should be distributed by a responsible employee who is not otherwise connected with any of the steps of payroll preparation.

Reason for Control

This will segregate the responsibility for processing payroll information from the distribution of payroll checks. In small local governments, employees can be required to call for their checks at a central location. In other governments, with a large number of employees and where the physical spread of work locations precludes central distribution, checks should be given out at the work station by someone who is not responsible for time and attendance reporting.

Reconciliation Procedures

6-6-1 Establish a separate bank account for payroll transactions.

Reason for Control

A separate bank account segregates net payroll checks, direct deposit transactions and withholding payments from other cash disbursements. The establishment of a separate bank account will ease the reconciliation of high volume payroll transactions and will also facilitate the identification of uncashed payroll checks.

6-6-2 Reconcile the payroll account monthly.

Reason for Control

Payroll is often one of the last bank accounts to be reconciled because it is generally a zero balance account. It is important to reconcile this account monthly so that uncashed payroll checks can be promptly identified and rectified.

6-6-3 The payroll bank reconciliation should be performed by an employee who is not connected with the authorization of payroll changes or with payroll preparation.

Reason for Control

Segregating reconciliation duties from authorization and preparation duties provides for an independent review of transactions that have been processed by the bank and of outstanding checks.

Statutory Controls

6-7-1 A complete payroll should be submitted timely to the appropriate civil service agency or officer for certification.

Reason for Control

Section 100 of the Civil Service Law provides, among other things, that the Department of Civil Service or "municipal commission" having jurisdiction must certify that "the persons named (on a payroll) are employed in their respective positions in accordance with law and rules made pursuant to law" prior to an officer "approving or paying any salary or compensation ..." Section 100 also contains provisions relating to the time frames for obtaining the certification. For further information concerning this requirement, you should contact the State Department of Civil Service or your local civil service agency or official.

Distinguishing Employees From Independent Contractors

Situations sometimes occur where it is not clear whether an individual who performs services for a local government is an employee or an independent contractor. When these situations occur, it will be important for the local government to have a process in place to assist in making an objective and defensible determination. Misclassifying an individual as an independent contractor rather than an employee can create a liability for interest and penalties on unpaid employment taxes. Conversely, misclassifying an independent contractor as an employee may result in extra costs for benefits the individual is not entitled to. Whether an individual is an officer or employee, or an independent contractor is dependent on numerous factors. Except for elected officials, the lack of civil service status generally should be considered a red flag that an employer/employee relationship may not exist. Documentation of the factors considered in these situations and the conclusions reached should be retained for audit purposes.

7-1-1 All new employee positions (including job descriptions) should be formally created and the approval of the appropriate civil service agency or officer obtained when required.

Reason for Control

This control not only fulfills civil service requirements, but also serves to distinguish between properly established employee positions and other types of business relationships. Civil service classifications are not established for independent contractor relationships. Hence, the lack of an established civil service position can be a leading indicator that an individual is an independent contractor rather than an employee.

7-1-2 Individuals should not be added to the payroll roster unless a vacant civil service position exists or the creation of a new position has been requested by the governing board or other appropriate body or official.

Reason for Control

The civil service system provides an established and recognized framework for creating new positions and certifying their legitimacy.

7-1-3 For all attorneys, physicians, engineers, architects, accountants, and auditors who were engaged on or after April 1, 2008 and who are determined to be "elected officials, public officers or employees," complete and file Retirement System Form RS 2414.

Reason for Control

New York State and Local Retirement System regulations require employers to certify the employment status of individuals employed in the above referenced professions. Form RS 2414 must be certified by the chief fiscal officer and returned to the Retirement System, along with supporting documentation. Form RS 2414 can be accessed at http://www.osc.state.ny.us/retire/forms/rs2414.pdf.

Equipment and Consumables

Local governments purchase a wide variety of equipment and consumables to assist in delivering services to taxpayers and other residents. "Equipment" includes highly visible (and easily trackable) items such as dump trucks, snow plows, and office equipment. It also includes highly portable items such as cameras, laptops, chain saws, and even lawn equipment. The term "consumables" generally refers to items such as gasoline, cafeteria food items, and copier paper. The design of controls put into place to protect these assets will vary depending on the value and the portability of the asset.

Equipment that is more easily lost or misused may need stronger controls. For example, items such as cameras, laptops, and tools may require stronger controls than heavy equipment, such as bulldozers and trucks. The relationship between the cost of implementing the control and the benefit to be achieved should be evaluated.

This section discusses internal controls that will help ensure that all acquisitions and dispositions of equipment and consumables are authorized and accounted for, and equipment and consumable items are properly controlled.

Equipment

Policy Considerations

8-1-1 The governing board should adopt a written policy that sets forth guidelines and procedures for establishing and maintaining controls over equipment. Subject to statutory requirements,[10] the policy should:

- Identify the major types of equipment and the persons or positions responsible for physically safeguarding these assets
- Establish a dollar threshold (or minimum cost) below which equipment will not be inventoried because of cost-benefit considerations
- Describe the types of inventory records that should be maintained and the persons or positions responsible for maintaining these records
- Require that the physical control over assets and the maintenance of inventory records be divided among different departments when possible
- Require that periodic physical inventories be conducted to compare inventory records to actual assets.

Reason for Control

Developing a formal written policy establishes guidelines for managers to follow when implementing procedures to safeguard equipment from misuse or theft.

[10] See e.g., Highway Law section 142(3), which requires the town superintendent of highways to annually make a written inventory of all machinery, tools, implements and equipment and to deliver the inventory to the town board on or before September thirtieth of each year.

Safeguarding Procedures

8-2-1 Mark or label all equipment as property of the local government. For more sensitive items, such as those susceptible to theft, tags with individual serial numbers should be affixed to the equipment and detailed records should be maintained. Label and/or tag equipment before it is placed into service.

Reason for Control

Generally, all equipment purchased must be placed under some level of control and safeguarding. For the larger, more cumbersome equipment such as desks and cabinets, the items should be identified with a tag showing that it belongs to the local government. The records should show the total number of items in particular areas of responsibility. For more sensitive items, tags with individual serial numbers should be affixed to equipment and detailed records should be maintained. Placing equipment into service prior to tagging increases the risk that the asset has not been recorded in the inventory records and that accountability for the equipment will not be established.

8-2-2 Assign responsibility for small, high-dollar value equipment such as laptops, projectors, and specialized hand tools to a specific employee. Safeguard highly portable equipment in limited access cabinets or storerooms when not in use.

Reason for Control

Small equipment and inventory are more easily lost or stolen. Making an employee accountable for their safeguarding and limiting access to these assets reduces the potential for loss or theft.

Inventory Records

8-3-1 Equipment inventory records should contain descriptions, quantities, locations, dates of purchase and original cost; when appropriate, assign responsibility for the asset to a specific official or manager.

Reason for Control

Detailed equipment records make verification of the existence of the equipment easier and demonstrate to employees that management is monitoring equipment purchases and use, thereby deterring theft and misuse. Assigning responsibility to a specific employee holds that person accountable for safeguarding equipment.

8-3-2 Subject to statutory requirements, the preparation and maintenance of inventory records for equipment should be assigned to an individual who does not have custody of the equipment.

Reason for Control

If the same person has custody of an asset and also maintains the inventory records, an opportunity exists for falsifying the inventory listing to disguise the theft or loss of a valuable asset.

Retirement/Disposal of Equipment

8-4-1 Retirement and/or disposal of equipment should be authorized and documented prior to the actual disposal of the items and their removal from the equipment inventory listing.

Reason for Control

Theft or other loss is easier to conceal if equipment can be removed from the records without prior written approval. In addition, prior approval ensures that only equipment that is unneeded, unusable, or obsolete is disposed of.

Physical Inventory Procedures

8-5-1 Annually, a physical inventory of equipment assigned to each location should be made. The inventory should be documented.

Reason for Control

A physical inventory verifies the existence of equipment.

8-5-2 The physical inventory should be compared to the prior physical inventory of equipment and to the detailed property records. All material differences should be identified and reviewed by management.

Reason for Control

Comparing inventories year-to-year and to property records will identify missing equipment, equipment disposed of without authorization and untagged equipment.

8-5-3 A periodic verification of the inventory listing should be conducted by someone who does not have custody of the asset.

Reason for Control

If the employee responsible for safeguarding assets is also responsible for verifying their existence, an opportunity exists to disguise the theft or loss of valuable assets.

Consumables

8-6-1 Consumable commodities such as gasoline, diesel fuel, copier paper, cafeteria foods, and supplies should be maintained in locked or controlled environments.

Reason for Control

Commonly used commodities such as the ones listed above are frequent targets for theft and misuse. By limiting access to these commodities, opportunities for theft are reduced.

8-6-2 The usage of gasoline and diesel should be tracked by vehicle and by the individual accessing the commodity. For stored gasoline and diesel, an electronic card system can be used to maintain accountability over the use of these commodities. In the absence of a card system, a manual record should be maintained of the dates and amounts of gasoline and diesel used, the vehicle receiving the fuel and whom it was pumped by.

Reason for Control

These commodities are highly transferable and, if they are not maintained in a controlled environment with accountability over their usage, their disappearance is difficult to track. Usage records, whether they are maintained manually or electronically, should also indicate who is using these commodities.

8-6-3 A reconciliation of fuel purchases, fuel usage, and fuel remaining on hand should be conducted periodically.

Reason for Control

A periodic reconciliation of purchases, usage, and fuel on hand will determine if significant amounts of fuel are unaccounted for.

8-6-4 For cafeteria supplies and goods, the cafeteria manager should maintain control over these commodities by limiting access to them. The cafeteria manager should also monitor the reordering of commodities to detect unusually high usage patterns.

Reason for Control

Restricting access to as few employees as possible will limit but not completely prevent the theft of food and cafeteria supplies. Monitoring reorder points for meats and other valuable food commodities may also help to detect excessive usage that may indicate the need for further investigation.

8-6-5 The disposal of expired or otherwise unusable food products should be properly authorized and documented by the cafeteria manager.

Reason for Control

Authorization and documentation discourages personnel from intentionally discarding usable inventory and then stealing the items.

Information Technology

This section of our guide is intended to address information technology (IT) risks and the types of internal controls that can be implemented to reduce these risks.

IT is involved in many aspects of local government operations, such as record keeping, banking, payroll, inventory monitoring and control, tax collection, and public safety. Safeguarding information needed for these types of services and support functions is challenging when records pertaining to these functions are created and stored on computers. A secure IT environment manages, processes, and protects computerized information. An inadequate IT environment can have a negative effect on operations that can contribute to the loss of sensitive information, theft, misuse of resources, inefficient use of taxpayer resources, and inaccurate information for decision makers. The risk of an inadequate IT environment exists whether IT administration is handled in-house, outsourced to vendors, or conducted through intermunicipal cooperation arrangements.

Establishing the IT Framework

9-1-1 The governing board or other authorized body or officer should establish a centralized IT administration for overseeing computer and network operations. Options include appointing a Chief Information Officer, establishing an IT department, or assigning IT oversight to an upper-level manager. Small units of local government may need to consider other options for administering the IT environment, such as intermunicipal cooperation or outsourcing.

Reason for Control

IT administration will communicate technology needs to executive management and the governing board, and be responsible for training users, enforcing security regulations, and ensuring all confidential data is secured.

9-1-2 IT administration should be in charge of and responsible for all IT matters and should report to executive management and the governing board.

Reason for Control

IT administration will assess technology needs, coordinate purchases and service contracts, and help ensure that security policies and procedures are uniformly implemented to protect IT assets and related data. All major technology decisions should go through executive management and the governing board.

9-1-3 IT administration should approve all new hardware (keyboards, monitors, servers[11]) and software (operating systems[12] and applications) acquisitions, with governing board consent for major acquisitions in accordance with legal requirements.

Reason for Control

It is important to obtain approval from IT administration on all acquisitions because some hardware and software may not be compatible with the network.[13] If a user adds equipment or applications without the IT administration's approval, it could put the network at risk.

9-1-4 Adopt a comprehensive IT security plan. Generally, security plans show the results of a risk assessment and explain what measures the local government will put in place to mitigate prioritized risks. The overall security plan should include a disaster recovery plan, back-up procedures, computer use policy, rules for the users' accounts, and a remote access policy.

Reason for Control

The security plan will help the local government implement measures to reduce IT risk by summarizing important aspects of the IT environment and providing a platform for further IT procedures and controls.

9-1-5 Disseminate the security plan to appropriate IT users.

Reason for Control

The policies included in this plan will allow the governing board to communicate its expectations and share its vision for the IT environment with all users.

[11] A server allows computers connected to the network access to data files, applications, and peripheral devices.

[12] An operating system is a program designed to run other programs on a computer. It is considered the backbone of a computer, managing both software and hardware resources.

[13] A network is a system of devices that communicate to each other (computers, servers, fax machines, and printers).

User Accounts

9-2-1 Establish procedures for creating, modifying, and deleting user accounts.

Reason for Control

These accounts identify users and establish relationships between a user and a network, computer or application, and contain passwords and access rights to files and applications. Having a unique user account allows users to gain access to their documents and files from any computer on the local government's network. Established procedures should include uniform guidance to be applied in relation to user accounts. This guidance should cover creation, modification or deletion of user accounts, access to user accounts and user account requirements.

9-2-2 Ensure all users have a unique user name.

Reason for Control

When each user has a unique name, access can be appropriately restricted and activities can be traced to the specific user. Shared user accounts should be prohibited. An example of a shared account is an account named "Business Office" that is used by more than one person located in the business office.

9-2-3 IT administration should only add users to the network after human resources, payroll, or other appropriate officers notify IT administration that they are legitimate users. The notification should be documented and retained.

Reason for Control

Controlling the addition of users to the network will ensure that users added are authorized and appropriate. Documentation should be available for future review or reference.

9-2-4 Human resources, payroll, or other appropriate officials should notify IT administration immediately when an individual's employment or contract is terminated so that IT administration can deactivate the user's access to all computer-related applications. This notification should be documented and retained.

Reason for Control

Revoking access to employees or IT contractors who leave service helps to ensure that they cannot alter, delete, or otherwise damage data or programs. Documentation allows management to monitor adherence to the policy.

9-2-5 Terminate dormant accounts (those that have not been used for a long period of time) on the network and in specific applications. IT administration should determine the length of inactivity that indicates a dormant account.

Reason for Control

A dormant account could indicate a user account is no longer associated with an active employee and is unnecessary for the performance of duties. Leaving such an account active could allow for inappropriate access by an unauthorized individual.

9-2-6 Use an authentication system to log-on to the network and specific applications. An authentication system forces the user to prove they are authorized to use the account by requiring them to type a password, insert a key card, or pass a biometric test.[14]

Reason for Control

Using an authentication system reduces the risk that unauthorized users can gain access to the network and its applications or data.

9-2-7 Passwords should contain complexity requirements. They should be at least eight characters and contain an uppercase character, a lowercase character, a numeric character, and a special character. They should not include the use of names or words that can be easily guessed or identified using a password-cracking mechanism, should be required to be changed periodically (every 30-90 days), and should not allow the last six passwords to be reused.

Reason for Control

The password requirements will make it more difficult for someone to inappropriately access a user's account.

9-2-8 Encourage users to refrain from writing down passwords.

Reason for Control

This control prevents others from viewing users' passwords and gaining inappropriate access to their user account.

9-2-9 Disguise passwords upon entry into the computer, such as showing asterisks on the screen when a password is typed in. Also, passwords that are stored in the network should be disguised.

Reason for Control

Nobody should be able to obtain a user's password (even IT administration). If a user forgets his or her password, IT administration can always reset it instead of retrieving the original password. This control is important to ensure the security of each user's account.

9-2-10 Require users to log off their account before stepping away from the computer and require users to shut off computers before they leave for the day.

Reason for Control

If a computer stays logged on and the user is not monitoring their computer, others can inappropriately use their account and access systems and data. Shutting off the computer will provide another layer of security and has the added bonus of saving electricity.

[14] Biometrics is the biological identification of the user and can include various types of equipment, such as eye or fingerprint scanners or voice recognition software.

9-2-11 Lock user accounts after three to seven consecutive attempts with an incorrect password.

Reason for Control

Unsuccessful attempts to gain access to an IT environment may reflect an intruder guessing the password of a user account. This control prevents an intruder from having unlimited guesses to a user's password. If a user forgets his or her password and locks out their account, IT administration will be able to reset the password and give them access to log on to their account.

9-2-12 Lock user accounts after a certain period of inactivity. There are usually settings that can be established that will lock the user's account after a specified period of time.

Reason for Control

If a computer stays logged on without the user present, others can inappropriately access the user's files or other data.

9-2-13 IT administration should give users access only to the areas of the applications (including within financial software) and the network they need to perform their job duties.

Reason for Control

Limiting access will ensure that only appropriate users are allowed into the applications, network and stored data. If users don't need access to sensitive data, don't give it to them.

9-2-14 IT administration must ensure that the default accounts for servers and applications are deleted, or at least that the passwords are changed.

Reason for Control

Servers and applications usually come with a default account already added to them so that someone can set up the network configuration. This account is usually the same username and/or password for each customer (which can sometimes be found online). If the account isn't deleted or the password isn't changed, anyone could penetrate the server or specific applications, often with high-level access rights, to make changes.

Monitoring Computer Users

9-3-1 Require employees and officers to sign a computer use policy. This policy should explain that information stored on government computers is not private; specify that computers should not be used for personal purposes, unless the policy allows for incidental personal use; and outline penalties for misuse of equipment, subject to collective bargaining agreements.

Reason for Control

Users need to understand what is expected of them. Having users sign the policy ensures that they are aware of the rules and accept responsibility if they do not follow them.

9-3-2 Monitor user access into the network.

Reason for Control

If users are logging in at unusual times (in the middle of the night or on weekends) or if there are numerous logged error messages (passwords input wrong), it could indicate a problem or an attempted attack by an intruder.

9-3-3 IT administration should use a web filter and review the logs it creates.[15]

Reason for Control

A web filter will reduce the amount of inappropriate websites users can access. In addition, reviewing the logs will help IT administration monitor how well users are complying with the computer use policy and possibly suggest other websites to block.

9-3-4 Review audit logs of the applications, including the financial software.[16]

Reason for Control

Applications normally contain multiple audit logs that can be reviewed to ensure individuals are making only authorized changes in the application. Any unusual or unauthorized activity could indicate a breakdown in controls or possible malfeasance.

[15] A web filter creates logs, or lists, of what websites users are accessing. It also blocks users from going to certain websites (those websites would ultimately be chosen by the IT administration, in consultation with executive management).

[16] Audit logs record certain activity in the application by user, generally with a timestamp. For example, an audit log could show that on March 13, 2010, at 11:13 am, user 12345 changed employee # 1234's hourly rate.

9-3-5 When audit logs or other red flags indicate possible improper computer use, executive management should consider having IT administration review a sample of users' hard drives at unannounced intervals.[17]

Reason for Control

Computer equipment may only be used for local government purposes and incidental personal use, if allowed by the local government's policy. Computer equipment should not be used for other than minor, incidental personal use. Periodic reviews of hard drives will reveal inappropriate usage such as downloaded games, music, or pictures that are of a personal or inappropriate nature.

9-3-6 Provide training to computer users on the use and protection of the IT assets related to the network.

Reason for Control

Computer users need to know exactly what is expected of them and how to perform what is expected of them to uphold a secure IT environment.

Data Security

9-4-1 Classify all local government data according to sensitivity, and when possible, segregate high and low sensitivity data on the network. If a public web server[18] is used for business purposes also, confidential information should be stored on a separate server.

Reason for Control

If users or the public need access to a local government's server, it is important to restrict access to confidential data so it cannot be viewed, altered, deleted, or stolen.

9-4-2 Encourage computer users to store all sensitive data on the network, not on their hard drives.

Reason for Control

Storing data on the network ensures that, if a user's computer breaks down, that data will not be lost and could be accessed from the network by logging on from another computer. Also, if a computer is lost or stolen, any sensitive data would not be available on that hard drive.

[17] The hard drive is the area on a computer where users store information such as music, pictures, documents, and games.

[18] A public web server is an online system that allows the public to have access to the local government's server (for example, accepting online payments).

9-4-3 If financial transactions are made through a public web server, use Secure Sockets Layer (SSL).[19] SSL is widely used to do two things: validate the identity of a website, and create an encrypted connection for sending credit card and other personal data.

Reason for Control

It is important to protect information input by a local government's customers (such as credit card and bank account numbers) so that others cannot access them.

9-4-4 Encrypt and/or password protect information that flows in and out of the system (through email or a portable device such as a data stick) or use portable devices that have password security.[20]

Reason for Control

Encryption provides another level of security for the data in case someone gains access to the email or device. Since the data is encrypted or password protected, the information may be kept inaccessible to unauthorized use.

9-4-5 If portable devices (for example data sticks) are shared among users, ensure all sensitive data is erased from the device before it is distributed to another user.

Reason for Control

Sensitive data should not be given to users who are not authorized to view it.

9-4-6 Ensure that all sensitive data is removed from devices being sent out for service or warranty work.

Reason for Control

To avoid inadvertent misuse, sensitive data should not be given to people who are servicing equipment. Recent news articles show that even items such as copiers and printers have hard drives in them that store sensitive information.

9-4-7 Use sanitizing software (which completely erases data) and/or physically destroy a computer's hard drive before disposing of computers.

Reason for Control

It is important to get rid of data on a computer before it leaves the local government so that unauthorized users do not see any sensitive information. Simply reformatting the hard drive before disposing of a computer does not completely erase the data.

[19] SSL is a cryptographic protocol (conversion of data into secret code, which is then turned back in to the original data by the receiver) that creates an encrypted connection for sending data.

[20] Encryption essentially takes the characters (like words and numbers) in sensitive data and transforms them into code. Only a user with the decryption device can unlock the code and transform the data back into understandable characters.

Software Security

9-5-1 Test software before general dissemination to computers. In addition, back up original files before installing new software in case data does not transfer properly.

Reason for Control

Testing software is essential because it ensures the software will work well with the local government's network. In addition, backing up files before the new software is uploaded will ensure that if something goes wrong with the upload, the original data will be available.

9-5-2 Only install software necessary for local government business.

Reason for Control

Personal software, even if for a governmental use, should not be installed on government computers because it would not have been tested on the network and could introduce viruses or other disruptions to the network.

9-5-3 Restrict rights to download or install software to as few individuals as practical.

Reason for Control

Software additions or changes should be made by IT administration, when practical, to ensure the software works well with the network, is safe to use, and is for business use.

9-5-4 IT administration should backup software by securing the master copies of the software and its user instructions.

Reason for Control

The local government most likely paid for the original documentation; if it is destroyed or lost, the government may have to pay for another set of instructions.

9-5-5 Give licensed software only to appropriate users who need it to perform their duties.

Reason for Control

The local government is responsible for the appropriate use of licensed software. For example, the local government may have purchased rights for only a certain number of users, and it may be inappropriate or violate the license agreement to disseminate to additional users.

9-5-6 Maintain an inventory of software applications installed on all computers.

Reason for Control

A software inventory is especially important if installation of software is not restricted. IT administration should be aware of what software is on each machine to ensure its appropriateness. In addition, maintaining a software inventory will help ensure there are no copyright infringements.

Network Security

9-6-1 Install an appropriate firewall.[21]

Reason for Control

Firewalls are tools the local government can use to monitor and stop intruders from accessing the network. Intruders could steal sensitive information or introduce viruses that could cripple the network if they are not stopped by a firewall. A firewall can also help ensure that users are not accessing websites that are not necessary for local government operations.

9-6-2 Install an intrusion detection system (IDS).[22]

Reason for Control

An IDS allows a local government to detect, monitor and stop intruders trying to access the network.

9-6-3 Periodically review activity logs recorded by the firewall and IDS.

Reason for Control

By reviewing the recorded activity and any potential intruders into the network, IT administration can determine if the firewall or IDS settings are appropriate and determine if changes are needed. Also, this will indicate potential attacks or other problems that need to be addressed.

9-6-4 Utilize virus protection and ensure all computers have an up-to-date version.[23]

Reason for Control

Viruses can damage both the computer and the network if not blocked in time. Up-to-date virus protection incorporates the latest known protections against ever-changing electronic threats.

9-6-5 Ensure updates to servers, the operating system, and applications are done timely.

Reason for Control

Vendors often discover vulnerabilities with or add features to their software or equipment and usually provide updates. These should be put on each computer or server as soon as possible to avoid potential intrusion attacks, prevent inappropriate access to data, and ensure efficient performance.

[21] A firewall accepts or denies traffic in and out of the network. It can stop an intruder from gaining unauthorized access to the network or prevent a user from looking at a prohibited website. The firewall should be capable of tracking all of the people who try to penetrate the network.

[22] An IDS inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise an IT environment.

[23] Virus protection is software that IT administration can install on each computer that will scan the hard drive and warn users that a potential virus exists on the computer or on a website that the user is trying to access.

9-6-6 IT administration should ensure there are no open ports on the servers.[24]

Reason for Control

It is important to restrict access to servers and other hardware only to authorized users to prevent someone from harming the network and inappropriately accessing its data.

9-6-7 If wireless access is used, ensure the wireless connection is authorized and protected (via password or encryption) so that people with other portable devices (PDAs, laptops, cell phones) cannot get on the network.[25]

Reason for Control

It is important to secure all connections to the network from users who are not authorized in order to prevent someone from harming the network and inappropriately accessing its data.

9-6-8 If a wireless access point is installed, change the default service set identifier (SSID) to something unique and change the default password to match the complexity requirements of the password policy in place. Disabling SSID broadcasting is also recommended.

Reason for Control

SSID is a name that identifies the wireless access point. Often the default name is the name of the vendor who manufactured the access point. By knowing the vendor name, an unauthorized person could search the Internet and obtain default administrative accounts and related passwords. The person could then attempt to log in to the access point and change settings or turn it off, without having legitimate administrative access. By not broadcasting the SSID, the government ensures that the wireless access point would stay hidden and not be easily detectable by unauthorized users.

9-6-9 Restrict remote access to those that who need it to perform their duties offsite. Ensure that all remote access is authorized prior to use and that users adhere to the local government's security policies.[26]

Reason for Control

Remote access can be allowed, but certain procedures should be in place to ensure the protection of the local government's network. Having a remote access policy will allow IT administration to establish a set of rules for those who wish to obtain remote access. Opening a local government's network to remote access to an excessive amount of users creates vulnerability and could provide access or data to an unauthorized user.

[24] Ports are pathways in or out of a computer or other network device and open ports automatically accept packets of information (allow communication). If a user was able to find or guess the IP address to a server which has open ports, they could put it in an address bar on a web browser and initiate communication to the server. Also, if the ports are left open and the server does not require a password, someone could then gain access to the server and make unauthorized changes to settings.

[25] Wireless access is used when a user wants to reach the Internet or other portion of the network without a cord being plugged into his or her computer..

[26] Remote access is when a user is allowed to access the local government's network from an off-site location.

9-6-10 Consider using a VPN (virtual private network) for remote access users.

Reason for Control

VPNs provide a secure means through which to transfer data between a remote user and the local government's network. A VPN further secures the connection between the remote user and the network in order to avoid inappropriate access to data being transmitted.

9-6-11 Control and monitor remote access by limiting access through ports and reviewing firewall or software audit logs.

Reason for Control

This control allows IT administration to control who is remotely accessing the network and to ensure that remote access users are accessing necessary applications.

9-6-12 If some or all of IT administration's duties are outsourced to a vendor, evaluate the risk of having this vendor access your network. The contract with the vendor should provide that the vendor sign an authorization form agreeing to services to be provided and stating they will follow the local government's security policies.

Reason for Control

Giving vendors access to a network increases the risk of improper manipulation of data or applications. Prescribing the agreed upon duties in advance under the contract and making a vendor sign a form gives the local government control over what the vendor is allowed to access in the network.

9-6-13 Ensure that vendor access to the network is restricted only to files and applications needed to perform their duties.

Reason for Control

Restricting vendors to necessary parts of the network will help ensure that they do not inappropriately access or damage other data or applications.

Physical Security

9-7-1 Lock up or otherwise secure servers and wiring closets. Limit access to those who need it, restrict access by keys or key cards, and monitor access.

Reason for Control

Limiting access only to authorized users of servers and wiring closets can help prevent unauthorized access to information, tampering with sensitive equipment, or theft.

9-7-2 Ensure servers and wiring closets cannot be reached from the outside by windows or doors. When feasible, consider using equipment to secure the room, such as window bars, an alarm system, motion detectors, or video cameras.

Reason for Control

Restriction of access to equipment will further ensure the safety of the servers and wiring closets from outside intrusion.

9-7-3 Server rooms and wiring closets should have proper environmental controls. This includes maintaining temperature and humidity in accordance with the manufacturers' specifications, protecting cabling and wiring from foot traffic, keeping equipment away from air conditioning and heating units, and banning food and drinks from these rooms.

Reason for Control

All of these protections reduce the possibility of environmental hazards such as fire, food, or water damage. In addition, if equipment overheats or is not kept at the proper humidity, it may be destroyed, or not operate for its expected life.

9-7-4 Install automatic and manual fire-suppression systems in the server rooms and wiring closets and periodically test them. In addition, IT administration should be trained in how to use the fire-suppression system.

Reason for Control

Installing and utilizing these systems properly may spare equipment in the case of a fire.

9-7-5 Plug all equipment into surge protectors and use an uninterrupted power supply (UPS) or a backup power source.

Reason for Control

Surge protectors protect equipment from being destroyed if there is a big surge in power (such as if lightning hits the power lines). UPS provides equipment with a backup source of power when normal utilities are not available and enables equipment to continue to be used and/or to be properly shut down.

9-7-6 Maintain and repair equipment as needed, either with in-house staff or outside vendors. If vendors are used, monitor and restrict access to the intended equipment.

Reason for Control

It is important to perform maintenance on the equipment to get as much useful life as possible out of it. In addition, monitoring vendors who come in to do repairs will reduce the risk that they are harming the network or inappropriately accessing its data.

9-7-8 The computer use policy should inform users how to secure laptops, such as by not leaving them unattended in their cars or in public places.

Reason for Control

Users need to know how to treat the local government's equipment so that it, or the data on it, is not lost or destroyed.

Service Continuity

9-8-1 Adopt a disaster recovery plan. The local government would carry out this plan in case of an emergency (such as a flood or fire) to resume orderly operations as soon as possible. This plan could include an alternate processing location[27] and a plan to procure computers with the appropriate software to resume normal operations.

Reason for Control

If an emergency occurs, this plan will help ensure the local government resumes its operations as quickly as possible.

[27] The alternate processing location is a place that the local government feels comfortable carrying out their normal business operations until they are able to resume work at their regular location, i.e., an empty warehouse or a nearby local government's facilities.

9-8-2 Test the disaster recovery plan to ensure it works as intended and that users know their duties during a disaster.

Reason for Control

Testing the disaster recovery plan provides an opportunity to discover any changes to the plan that need to be made to ensure that it works as intended.

9-8-3 Adopt a policy for backing up data. The policy should indicate how often and to what extent backups will be performed, how many backups will be maintained, and if backups will be incremental or complete.[28]

Reason for Control

Backups are essential tools to ensure data is available in case the original data is destroyed or inaccessible.

9-8-4 Maintain a list that describes each time a backup was performed and the type of backup that took place.

Reason for Control

A record of backups will help facilitate a restoration in the event that data is lost, and allows a supervisor to ensure backups are being performed and maintained properly.

9-8-5 Backup sensitive data with encryption.

Reason for Control

Encrypting backups of sensitive data makes it harder for unauthorized users to get access to the sensitive data if backups or lost or stolen.

9-8-6 Store backups at a secured, off-site location.

Reason for Control

Off-site storage is important because it will allow for a restoration of data even if the original data or worksite is destroyed.

9-8-7 Periodically restore backups.

Reason for Control

Periodic restoration ensures the restoration process works as intended and that the central administration is able to recover data if needed.

[28] Incremental backup means that only updates to the data are backed up, while a complete backup makes a backup of all the data. A good backup policy may include each of these styles done at different times. For example, an incremental backup could be done daily and a complete backup could be done at the end of each week.

Outsourced Services

Local governments sometime outsource certain financial or related functions to third-party specialists, also referred to as "service organizations." Some of the functions outsourced by local governments, subject to legal requirements and limitations, include:

- Payroll processing
- Accounting (commonly found in school districts utilizing a BOCES central business office)
- IT installation, maintenance, and/or management (commonly found in school districts utilizing a BOCES Regional Information Center)
- E-commerce implementation, maintenance, and/or fee collections
- Community Development Block Grant administration
- Third-party insurance administration
- Property tax or utility billing and collection services
- Ambulance or EMS billing and collection services.

Not every type of financial or related function may be outsourced and, even if authorized, a local government may be limited as to the type of third party with which it may contract or the particular aspects of a function that may be "outsourced." For example, local governments cannot outsource the collection of real property taxes other than to banks or trust companies.[29] And, generally, check signing authority cannot be outsourced to any other individual or organization. In addition, the outside contract would be subject to competitive bidding requirements, or if exempt from bidding (e.g., a professional service), subject to the local government's procurement policies and procedures.[30] Before you outsource, consult your legal counsel about the impact of existing laws on the financial or related function or service you plan to outsource.

Local governments that contract out finance-related functions must ensure that the service organizations are properly performing those functions. Local officers should also ensure that adequate internal controls are in place at the service organization to safeguard sensitive and confidential data, to protect public assets from loss or misuse, and to provide assurance that transactions are complete and accurately accounted for.

[29] Real Property Tax Law § 996 provides that a bank or trust company that has entered into an agreement with a municipality, pursuant to that section, to collect taxes on the behalf of the municipality is liable to the municipality for certain losses or damages, and is liable to taxpayers under certain circumstances. Not every function that may be "outsourced," however, is governed by a statute that prescribes statutory liabilities upon the third party.

[30] For additional information about competitive bidding requirements and procurement policies and procedures see our Local Government Management Guide entitled Seeking Competition in Procurement available on the web at: http://www.osc.state.ny.us/localgov/pubs/lgmg/seekingcompetition.pdf

Authorization Procedures

10-1-1 Ensure that written agreements are in place specifying the roles and responsibilities of the service organization and the local government.

Reason for Control

Written agreements define the contractual relationship and responsibilities between the service organization and the local government, including what services will be provided, when they will be provided, how they will be provided and at what cost. A written agreement should also stipulate that the service organization will have in place a system of internal controls to provide reasonable assurance that the local government's information will be protected against loss, abuse and fraudulent activity, even if not otherwise required by law. Written agreements should also require that all service organization audit reports will be provided to the local government.

Verification Procedures

10-2-1 Verify (on a test basis) that source data provided to the service organization has been processed correctly. For example, verify that the correct hours worked, leave credits used and pay rates have been accurately processed by the service organization.

Reason for Control

If reports, accounting records or other output prepared by the service organization are not regularly compared to a sample of source documents or source data, the reliability of work performed by the service organization will be unknown. Periodic verifications ensure that the accuracy of records and reports produced by the service organization meets the expectations of the local government.

10-2-2 If exception reports are available, local government personnel should review flagged items and recommend corrections, if necessary. Local governments should also consider setting the parameters for exception reports. For example, a bi-weekly gross payroll amount in excess of $1,000 (or another amount) could be set as the limit above which an exception item would be generated.

Reason for Control

Exception reports are a good tool for detecting errors or anomalies that occur in the processing of transactions or in the preparation of financial reports. Both the local government and the service organizations should review exception reports to limit the occurrence of errors in the output produced by the service organization.

Reconciliation Procedures

10-3-1 Perform reconciliations between source documents submitted to the service organization and output generated. For example, compare the total gross payroll amounts submitted for processing to the sum of net payroll checks and other disbursements.

Reason for Control

Reconciliation procedures that verify or compare total amounts expected to be processed to actual output help to ensure that all transactions have been processed correctly.

Reports

10-4-1 Review audit reports prepared for the service organization.

Reason for Control

Audit reports provide information about the financial condition of the service organization and any significant deficiencies in internal control identified by the auditors. If available, a SAS 70 audit report will also provide additional information regarding the design and effectiveness of the service organization's internal controls.[31]

[31] A SAS 70 report provides information and limited assurance regarding specific control objectives and procedures at a service organization. A SAS 70 report may also provide information about specific control deficiencies at the service organization. A SAS 70 report is an auditor-to-auditor communication and enables auditors of user organizations (such as local governments) to obtain an understanding of the service organization's internal controls and information system. Service organizations generally are not required to furnish SAS 70 reports but most large, commercial service organizations will have these reports available for review upon request by the local government.

Service Organization Internal Controls

10-5-1 Service organizations should provide documentation regarding their controls governing access to computerized data and the methods they use to monitor the effectiveness of these controls.

Reason for Control

Controlling access to data, especially personal and confidential data, is imperative in today's electronic environment. Local government management must ensure that data provided to a service organization is protected from both external and internal intrusions.

10-5-2 Service organizations should detail their procedures for preventing and detecting unauthorized financial transactions from occurring and not being detected.

Reason for Control

The risk of fraud occurring and not being detected is not lessened by having transactions processed externally. Local government management should inquire about fraud detection procedures used by the service organization, including the scope and frequency of internal audits.

10-5-3 Service organizations should provide information about the frequency of backups, the existence of off-site storage, the length of time that historical data is retained, and the ownership of backup data if the contract with the service organization is not renewed.

Reason for Control

When transactions are processed externally, the storage of data may also occur externally. Local governments must ensure that data provided to and processed by service organizations is protected from both external and internal intrusions and is accessible to the local government.

10-5-4 Service organizations should be required to provide proof of insurance to indemnify the local government against errors and frauds committed by the service organization's employees, even if not otherwise required by law.

Reason for Control

The actions of certain officers and employees of local governments are covered by "faithful performance bonds," but this coverage does not extend to transactions processed externally by another organization. Service organizations should be required to carry similar insurance as part of the contractual agreement with the local government.

Appendix A

How to Prepare a Bank Reconciliation

A reconciliation system is essential for maintaining proper control over cash. A bank reconciliation is a schedule showing and explaining the differences between the bank's records of cash accounts and the local government's accounting records. It helps account for transactions not yet recorded by the bank (i.e., outstanding checks) and transactions processed by the bank (i.e. wire transfers) that might not yet be recorded in the local government's books. It can also reveal errors made by either the bank or the local government. Book and bank balances should be reconciled monthly. Following are the steps to be taken:

1. Begin reconciliation by recording the book balances (from the accounting records) and the bank balance (shown on the monthly bank statement).
2. Arrange paid checks in numerical sequence.
3. Compare paid checks with the list of checks outstanding at the end of the previous month.
4. Prepare a list of checks that have not cleared the bank.
5. Fill out the adjustments to the book and bank balances as shown below. If the balances differ, follow steps 6 to 9.
6. Determine any charges or credits on the bank statements that have not been entered in the accounting records. A general journal entry may be needed to reflect this activity.
7. Trace deposits from the cash receipt journal to the bank statements. List any deposits not credited by the bank.
8. Compare paid checks with checks issued during the month.
9. If the amounts still do not balance, start the process from step 1 again.

Differences resulting from timing issues will eventually be recorded by the bank and require no actions. Unrecorded bank transactions or errors made by the local government may require adjusting entries. Banks will have to be notified of any errors on their part.

Sample Bank Reconciliation

Book Balances				
General Fund		$3,694.33		
Water Fund		927.78		
Sewer Fund		763.84		
Balances @ 1/31/XX			$5,385.95	
Less: NSF checks returned by the bank but not adjusted on books			**(36.65)**	
Adjusted Book Balance				**$5,347.30 ***
Bank Balances 1/31/XX:			$5,535.80	
Plus: Deposits In Transit (entered by bank 2/1/XX)			78.58	
			5,614.38	
Less: Outstanding Checks	#463	$51.34		
	#489	68.19		
	#501	147.55		
			(267.08)	
Adjusted Bank Balance @ 1/31/XX				**$5,347.30 ***

* When the adjusted book and bank balances do not agree, the reason for the difference should be researched and corrections should be made.

Division of Local Government and School Accountability

Central Office Directory

Andrew A. SanFilippo, Executive Deputy Comptroller

(Area code for the following is 518 unless otherwise specified)

Executive 474-4037
Nathaalie N. Carey, Assistant Comptroller

Audits, Local Government Services and Professional Standards 474-5404
(Audits, Technical Assistance, Accounting and Audit Standards)

Local Government and School Accountability Help Line ..... (855)478-5472 or 408-4934
(Electronic Filing, Financial Reporting, Justice Courts, Training)

New York State Retirement System

Retirement Information Services

Inquiries on Employee Benefits and Programs 474-7736

Bureau of Member Services 474-1101

Monthly Reporting Inquiries 474-1080

Audits and Plan Changes 474-0167

All Other Employer Inquiries 474-6535

Division of Legal Services

Municipal Law Section 474-5586

Other OSC Offices

Bureau of State Expenditures 486-3017

Bureau of State Contracts 474-4622

Mailing Address for all of the above:

Office of the State Comptroller,
110 State St., Albany, New York 12236

email: **localgov@osc.state.ny.us**

Division of Local Government and School Accountability

Regional Office Directory

Andrew A. SanFilippo, Executive Deputy Comptroller

Nathaalie N. Carey, Assistant Comptroller (518) 474-4037

Cole H. Hickland, Director • **Jack Dougherty**, Director
Direct Services (518) 474-5480

BINGHAMTON REGIONAL OFFICE - H. Todd Eames, Chief Examiner
State Office Building, Suite 1702 • 44 Hawley Street • Binghamton, New York 13901-4417
Tel (607) 721-8306 • **Fax** (607) 721-8313 • **Email:** Muni-Binghamton@osc.state.ny.us
Serving: Broome, Chenango, Cortland, Delaware, Otsego, Schoharie, Sullivan, Tioga, Tompkins counties

BUFFALO REGIONAL OFFICE – Robert Meller, Chief Examiner
295 Main Street, Suite 1032 • Buffalo, New York 14203-2510
Tel (716) 847-3647 • **Fax** (716) 847-3643 • **Email:** Muni-Buffalo@osc.state.ny.us
Serving: Allegany, Cattaraugus, Chautauqua, Erie, Genesee, Niagara, Orleans, Wyoming counties

GLENS FALLS REGIONAL OFFICE - Jeffrey P. Leonard, Chief Examiner
One Broad Street Plaza • Glens Falls, New York 12801-4396
Tel (518) 793-0057 • **Fax** (518) 793-5797 • **Email:** Muni-GlensFalls@osc.state.ny.us
Serving: Albany, Clinton, Essex, Franklin, Fulton, Hamilton, Montgomery, Rensselaer, Saratoga, Schenectady, Warren, Washington counties

HAUPPAUGE REGIONAL OFFICE – Ira McCracken, Chief Examiner
NYS Office Building, Room 3A10 • 250 Veterans Memorial Highway • Hauppauge, New York 11788-5533
Tel (631) 952-6534 • **Fax** (631) 952-6530 • **Email:** Muni-Hauppauge@osc.state.ny.us
Serving: Nassau, Suffolk counties

NEWBURGH REGIONAL OFFICE – Tenneh Blamah, Chief Examiner
33 Airport Center Drive, Suite 103 • New Windsor, New York 12553-4725
Tel (845) 567-0858 • **Fax** (845) 567-0080 • **Email:** Muni-Newburgh@osc.state.ny.us
Serving: Columbia, Dutchess, Greene, Orange, Putnam, Rockland, Ulster, Westchester counties

ROCHESTER REGIONAL OFFICE – Edward V. Grant Jr., Chief Examiner
The Powers Building • 16 West Main Street – Suite 522 • Rochester, New York 14614-1608
Tel (585) 454-2460 • **Fax** (585) 454-3545 • **Email:** Muni-Rochester@osc.state.ny.us
Serving: Cayuga, Chemung, Livingston, Monroe, Ontario, Schuyler, Seneca, Steuben, Wayne, Yates counties

SYRACUSE REGIONAL OFFICE – Rebecca Wilcox, Chief Examiner
State Office Building, Room 409 • 333 E. Washington Street • Syracuse, New York 13202-1428
Tel (315) 428-4192 • **Fax** (315) 426-2119 • **Email:** Muni-Syracuse@osc.state.ny.us
Serving: Herkimer, Jefferson, Lewis, Madison, Oneida, Onondaga, Oswego, St. Lawrence counties

STATEWIDE AUDIT - Ann C. Singer, Chief Examiner
State Office Building, Suite 1702 • 44 Hawley Street • Binghamton, New York 13901-4417
Tel (607) 721-8306 • **Fax** (607) 721-8313

New York State
Office of the State Comptroller
Division of Local Government and School Accountability
110 State Street, 12th Floor • Albany, New York 12236