The Practice of Internal Controls

Cornell Municipal Clerks School
July 16, 2014
Cash Receipts (Collection procedures)

- Centralize cash collections within a department or for the local government as a whole, when possible.
- Assign a separate cash drawer to each employee responsible for collecting cash.
- Restrictively endorse checks as soon as they are received.
- Instruct collectors that personal or payroll checks cannot be cashed from moneys in their cash drawers.
- Instruct collectors not to accept checks for amounts over the amount due.
Cash Receipts
(Collection procedures)

• 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.

• 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.
Cash Receipts (Collection procedures)

- 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.”
Cash Receipts (Deposit procedures)

- Secure deposited 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.
- Deposit cash timely.
- Deposit cash receipts intact.
- 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.
Cash Receipts
(Deposit procedures)

• The person who performs the bank reconciliation should be the final custodian of all deposit slips.

• The governing board should establish a charge for checks returned for non-sufficient funds (NSF). Notification of the NSF check charge should be included on all billings and posted in public view.
Cash Receipts (Record-keeping procedures)

- Record receipts in the accounting system timely.
- 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”).
- Employees responsible for collecting cash and preparing bank deposits should not record cash transactions in the accounting records.
Payroll (Authorization procedures)

• 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.).

• The terms and conditions of collective bargaining agreements should be clearly communicated to those responsible for payroll processing.
Payroll
(Authorization procedures)

• 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.

• Limit access to computerized payroll applications and data files containing potentially confidential information such as social security numbers and deductions.
Payroll (Payroll change procedures)

• 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.

• If payroll forms are used, control access to these forms by keeping them in a locked cabinet or drawer.
Payroll
(Payroll change procedures)

• 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.
Payroll
(Time and attendance records)

• 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.

• 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.
Payroll
(Time and attendance records)

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

• 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.

• Maintain leave accrual records and communicate leave balances to employees regularly.
Payroll
(Verification procedures)

• 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 persons listed on the payroll and that days and hours worked are accurate and justified.
Payroll
(Verification procedures)

• 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).
Payroll
(Payroll check procedures)

• Payroll checks should not be distributed to employees prior to the actual pay dates.

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

• Requests for direct deposit should be made in writing and kept on file for audit purposes.
Payroll
(Payroll check procedures)

• 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.

• Paychecks should be distributed by a responsible employee who is not otherwise connected with any of the steps of payroll preparation.
Payroll (Reconciliation procedures)

• Establish a separate bank account for payroll transactions.

• Reconcile the payroll account monthly.

• The payroll bank reconciliation should be performed by an employee who is not connected with the authorization of payroll changes or with payroll preparation.
Payroll (Statutory controls)

• A complete payroll should be submitted timely to the appropriate civil service agency or officer for certification.
Information Technology (Establishing the it framework)

- 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.

- IT administration should be in charge of and responsible for all IT matters and should report to executive management and the governing boards.
Information Technology
(Establishing the it framework)

• IT administration should approve all new hardware (keyboards, monitors, servers) and software (operating systems and applications) acquisitions, with governing board consent for major acquisitions in accordance with legal requirements.

• 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.

• Disseminate the security plan to appropriate IT users.
Information Technology (User Accounts)

• Establish procedures for creating, modifying, and deleting user accounts.

• Ensure all users have a unique user name.

• 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.
Information Technology
(User Accounts)

• 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.

• 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.
Information Technology (User Accounts)

- 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.

- Passwords should contain complexity requirements. They should be at least eight characters and contain an uppercase character, 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.
Information Technology (User Accounts)

• Encourage users to refrain from writing down passwords.

• 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.

• 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.

• Lock user accounts after three to seven consecutive attempts with an incorrect password.
Information Technology (User Accounts)

• 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.

• 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.

• IT administration must ensure that the default accounts for servers and applications are deleted, or at least the passwords are changed.
Information Technology
(Monitoring computer users)

• 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.

• Monitor user access into the network.

• IT administration should use a web filter and review the logs it creates.

• Review audit logs of the applications, including the financial software.
Information Technology
(monitoring computer users)

• 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.

• Provide training to computer users on the use and protection of the IT assets related to the network.
Information Technology (Data security)

• 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 is used for business purposes also, confidential information should be stored on a separate server.

• Encourage computer users to store all sensitive data on the network, not on their hard drives.

• If financial transactions are made through a public web server, use Secure Sockets Layer (SSL). 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.
Information Technology
(Data security)

• 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.

• 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.

• Ensure that all sensitive data is removed from devices being sent out for service or warranty work.

• Use sanitizing software (which completely erases data) and/or physically destroy a computer’s hard drive before disposing of computers.
Information Technology (software security)

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

• Only install software necessary for local government business.

• Restrict rights to download or install software to as few individuals as practical.

• IT administration should backup software by securing the master copies of the software and its user instructions.
Information Technology
(Software security)

• Give licensed software only to appropriate users who need it to perform their duties.

• Maintain inventory of software applications installed on all computers.
Information Technology
(Network security)

- Install an appropriate firewall.
- Install an intrusion detection system (IDS).
- Periodically review activity logs recorded by the firewall and IDS.
- Utilize virus protection and ensure all computers have an up-to-date version.
- Ensure updates to servers, the operating system, and applications are done timely.
- IT administration should ensure there are no open ports on the servers.
Information Technology
(Network security)

• 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.

• 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.

• Restrict remote access to those that 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.
Information Technology
(Network security)

• Consider using a VPN (virtual private network) for remote access users.

• Control and monitor remote access by limiting access through ports and reviewing firewall or software audit logs.

• 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.

• Ensure that vendor access to the network is restricted only to files and applications needed to perform their duties.
Information Technology
(Physical security)

• 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.

• Ensure servers and wiring closets cannot by 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.

• Server rooms and wiring closets should have proper environmental controls. This includes maintaining temperature and humidity in accordance with the manufacturer’s 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.
Information Technology (physical security)

- 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.

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

- 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.

- 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.
Information Technology
(Service continuity)

- 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 and a plan to procure computers with the appropriate software to resume normal operations.

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

- 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.
Information Technology (Service continuity)

- Maintain a list that describes each time a backup was performed and the type of backup that took place.
- Backup sensitive data with encryption.
- Store backups at a secured, off-site location.
- Periodically restore backups.