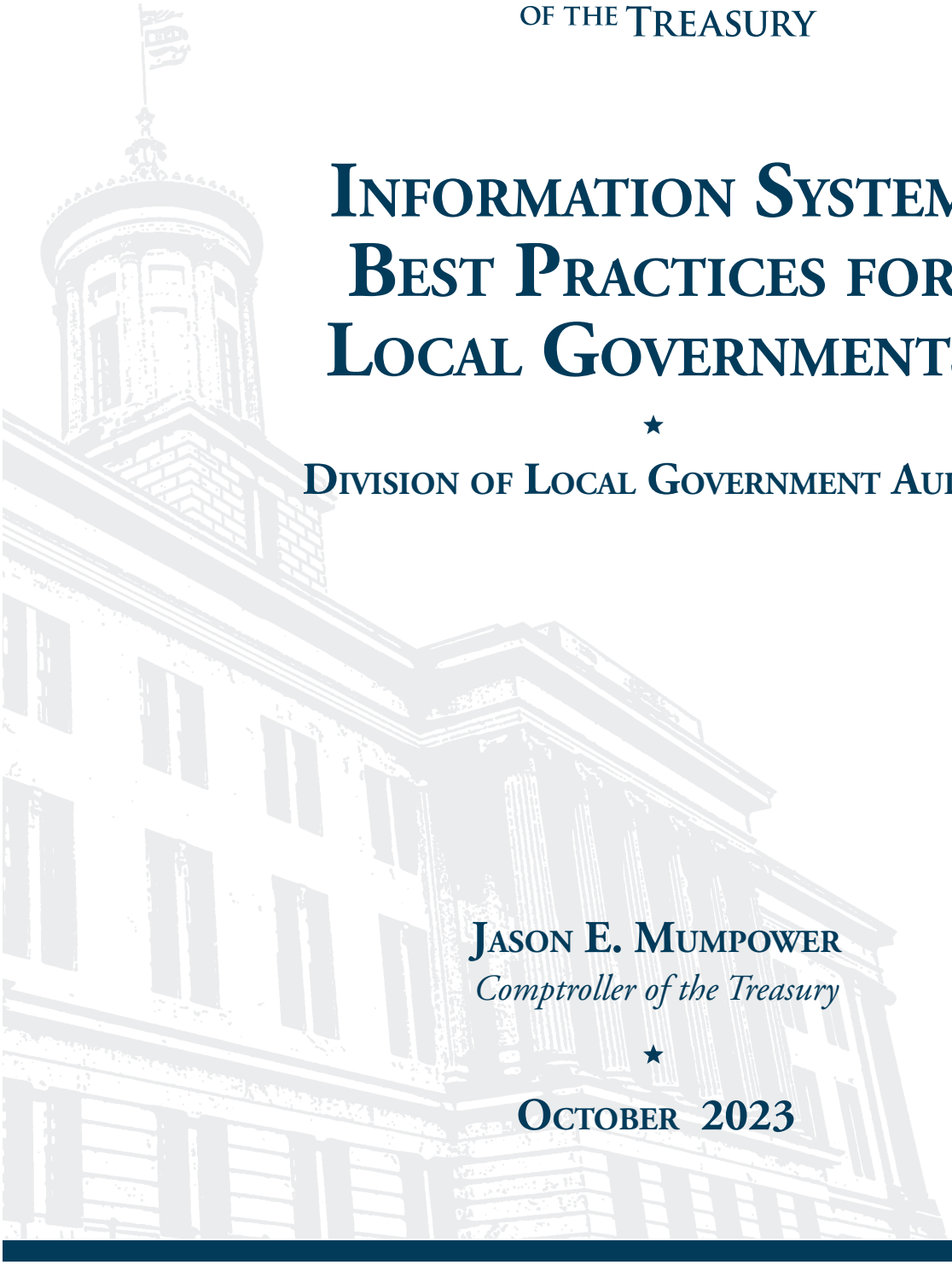

TENNESSEE COMPTROLLER OF THE TREASURY

Information System Best Practices for Local Governments

★

Division of Local Government Audit

Jason E. Mumpower
Comptroller of the Treasury

★

October 2023

Table of Contents

Purpose

The Comptroller of the Treasury Division of Local Government Audit establishes the following Information System (IS) Best Practices to provide practical information to local government officials about internal controls and encourage these officials to develop, implement, and maintain IS policies and procedures that conform to current best practices. While this document is intended to establish minimum levels of compliance for auditing purposes, it is not all-inclusive. Because the IT environment is dynamic and ever-changing, these guidelines will be modified periodically to reflect industry changes as closely as possible.

Introduction

General and application controls are the two main types of control activities applicable to the IS environment. All IS controls throughout industry may be broadly categorized as such and are presented here as follows:

Part One: General Controls
General Controls are established to provide reasonable assurance that the information technology in use by an entity operates as intended to produce properly authorized, reliable data when needed and that the entity is in compliance with applicable laws and regulations.

Part Two: Application Controls
Application Controls relate to the transactions and data produced by each computer-based automation system; they are, therefore, specific to each application. Application controls should be designed to ensure confidentiality, completeness, and accuracy of accounting records and the validity of entries made.

Part Three: Other Technology Issues
These are other technology related matters that should be properly addressed by local governments.

IS Management/Oversight

1. Develop policies and procedures related to the office's information systems.
    a. Ensure that the following items are documented:
        1. System startup/shutdown
        2. Operating system/application security
        3. System backup procedures
        4. Hardware disposition
        5. Virus prevention
        6. Routine processing of applications
        7. Planning and budgeting of IS operations
        8. Output distribution
    b. Distribute the policies and procedures document to all employees.
    c. Review and update the document at least annually.

2. Develop use agreements for all county information systems.
    a. Address password confidentiality in the agreement.
    b. Address employees' ability to remotely access the office's computer resources.
    c. Require all users to sign the agreement and maintain original agreements in the office.

3. Develop policies and procedures for systems development and program changes if software is developed by the county internally.
    a. Utilize a standard systems development methodology.
    b. Establish a procedure for change requests (e.g., request forms, authorizations, user acceptance)
    c. Document how program source code is controlled.

4. Request and review a Service Organization Controls (SOC) report if a service organization is used to host software applications. This report should be a SOC 1 Type 2 or SOC 2 Type 2 report. This report should examine the controls in place at the hosting organization.

5. Establish and maintain a formal cybersecurity awareness program that ensures end users are aware of current cybersecurity threats, the importance of protecting assets, and the related risks.
    a. Provide training to employees via presentations at educational events or videos or other information presented on cybersecurity websites such as COT Cyber Aware.
    b. Discuss current threats. Examples of relevant topics include but are not limited to:
        - Limiting the types of sensitive information collected, transported, and stored
        - Hazards of viruses, malware, ransomware, and spyware
        - Accessing malicious web sites
        - Downloading files from the Internet or simply clicking links
        - Embedded email links and downloading attachments that may appear reasonably valid

Physical Access Security

1. Ensure computer hardware is located in a secure area that is adequately ventilated.

2. Ensure access to the computer system is adequately controlled by door locks, security code locks, or other devices. Only appropriate individuals should have access. Keys should be returned or codes changed when individuals leave service. All visitors should be escorted or remain in sight of employees.

3. Ensure fire prevention and suppressions measures are in place. Fire extinguishers or other suppression devices should be present and should be routinely inspected.

4. Minimize the risk of power outages by using surge protection and uninterruptable power supply.

5. Store any negotiable documents in a secured location when not in use.

Operating System Security

1. Ensure operating system updates are installed on all computers when they become available.

2. Establish policies requiring that passwords be assigned to all accounts. These passwords should not be publicly displayed. Multifactor authentication could also be used to reduce security risks.

3. Implement password-protected screensavers or configure sleep mode settings so that the workstations require a password after no more than 30 minutes of inactivity.

4. Disable or rename all guest accounts.

Malware Detection

1. Install software on all servers and workstations that is designed to detect viruses and other malware.

2. Ensure the software is configured to install updated definitions as they become available.

System Backup Procedures

1. Develop backup procedures for all computer systems and communicate these procedures to staff.

2. In accordance with Section 10-7-121, Tennessee Code Annotated, a daily backup of data should be performed to physical storage media or an offsite/cloud location that is not connected to the production environment. If physical storage media is used, backups should be rotated to a secure, off-site location on a weekly basis. Possible locations include a vault at another county office building or a safety deposit box at a local bank.

3. If daily backup media does not include yearly information, perform a year-end backup as well. This media should be properly labeled and maintained at a secure off-site location for a period of 3 years.

4. Maintain a backup log of physical storage media that includes information such as the date of backup, media label, and storage location. The log should also note the individual performing the backup and whether they verified that it was successful.

5. Test backup information at least yearly to ensure the system can be successfully restored.

Disaster Recovery Planning

1. Document a plan that, at a minimum, addresses the following:
    a. A checklist to follow in the event the computer system is inoperable
    b. Hardware/software vendor and employee contact information
    c. Location of off-site backup information
    d. Specific contingency site location
    e. Inventory of hardware and software
    f. Manual processing procedures to follow until system is restored
    g. Comfort letter from vendor (if applicable)

2. Store a copy of the plan in an off-site location that would be accessible in the event of a disaster. A copy should also be provided to office personnel.

3. Ensure that the plan is updated annually.

4. Review the plan with office personnel at least annually and consider conducting a tabletop exercise to discuss a test scenario.

Wireless Network Security

1. Establish physical security controls over wireless network devices such that all devices are kept in an area only accessible to authorized individuals.

2. Ensure that the router password is changed from the default value.

3. Ensure the service set identifier (SSID) is not publicly broadcast and that encryption is used to require a password to access the network.

Application Access Controls

1. Establish policies that require each user to have a unique username and password for accessing software applications. Multifactor authentication could be used to reduce security risks.

2. Establish user security access on the principle of least privilege. Users should only have access to those functions that are necessary to accomplish their job responsibilities.

3. Ensure passwords remain confidential. Passwords should not be written down or shared with other employees. A password list should not be maintained. Passwords should not be saved in the browser.

4. Require passwords to be changed at least every 90 days.

5. Remove or disable usernames of former employees as soon as they separate from service.

6. Establish a policy requiring users to exit applications when away from their workstation for an extended period of time and after work hours.

Application Software Controls

1. Examine software functionality to determine if a proper audit trail is maintained within the software applications. Examples of functionalities to examine include the following:
    a. Alterations or deletions of receipts
    b. Removal or adjustments of customer accounts
    c. Alterations or deletions of general ledger entries
    d. Assignment of sequential receipt numbers

2. Establish procedures to review any audit logs or reports that display voids, alterations, adjustments, or deletions of transactions.

3. Ensure accounting software requires the closure of accounting periods within 60 days of period end.

Other Technology Issues

Cybersecurity Posture

1. Evaluate and regularly reassess the office's cybersecurity posture. Because many local government offices work closely with a vendor or local IT personnel to maintain their computer systems, they may need to be contacted to aid in this assessment. Examples of areas to consider include the following:
    a. Properly patching operating systems, software, and databases
    b. Properly updating virus definitions
    c. Properly configuring firewalls
    d. Ensuring backup information is not susceptible to attack

2. Consider acquiring insurance policies that provide coverage for cyberattacks. Understand the provisions of the policy and be aware of any exclusions.

3. Develop a cybersecurity response plan. Being prepared to respond to an attack will reduce the impact on office operations. Review the plan with office personnel and encourage them to promptly report any suspicious activity. Consider addressing the following in the plan:
    a. Inventory of all data and its location
    b. Instructions for immediate action after noticing potential attack
    c. Contact information for IT personnel/vendor
    d. Need to contact law enforcement, insurance providers, or other partners
    e. Need to notify parties that may have had personally identifiable information compromised
    f. Activation of disaster recovery plan

Required Filings

1. Ensure that statements are filed with the Comptroller of Treasury as required by Section 47-10-119, Tennessee Code Annotated. This statute requires that local governments using an electronic business system that provides for the sending/receiving of electronic records that contain electronic signatures or authorizations file a pre and post implementation statement. A common example would be the acceptance of online payments.

2. Ensure that statements are filed with the Comptroller of Treasury as required by Section 4-30-103, Tennessee Code Annotated. This statute requires that local governments implementing new technologies file a statement. A common example of a new technology would be remote deposit capture.

3. Ensure that statements are filed with the Comptroller of Treasury as required by Section 10-7-123, Tennessee Code Annotated. This statute requires that local governments who provide remote electronic access to records file a statement 30 days prior to offering this service.