



STATE OF TENNESSEE

John G. Morgan

COMPTROLLER OF THE TREASURY

Comptroller

STATE CAPITOL

NASHVILLE, TENNESSEE 37243-0264

PHONE (615) 741-2501

FOR IMMEDIATE RELEASE: October 4, 2006

CONTACT: Sherry Kast, Communications Officer, (615) 401-7806

Comptroller of the Treasury offers county governments guidance in identifying technology weaknesses

Nashville, TN – In an effort to help county governments address high risk areas involving their information systems, the Comptroller of the Treasury, Division of County Audit, has identified the top ten technology weaknesses as evidenced in recent technology audits.

In a recently released guide, “High Risk Areas Involving Technology in County Governments,” County Audit summarizes each high risk area and provides a recommendation for counties to help them address the weaknesses.

“In addition to conducting county financial and compliance audits, technology audits are now required,” said Art Alexander, director for the Division of County Audit. “By identifying high risk areas involving technology, the Comptroller’s Office is taking a proactive role in helping county governments identify areas that are vulnerable to fraud, waste, abuse and mismanagement.”

The weaknesses have been ranked in order of potential risk.

1. **Deletion of receipts.** Some applications provide users with the ability to delete and/or alter previously issued receipts leaving no evidence of the original receipt. An audit log that records all deletions or alterations is recommended as an alternate control.
2. **Segregation of duties.** Without segregation of duties an individual who receipts collections, maintains accounting records, reconciles bank statements, prints reports and signs checks could misappropriate funds without anyone’s knowledge. When adequate segregation is not feasible, management should take a more active role in reviewing transactions and reports.
3. **Hardware disposal.** In order to prevent someone from obtaining sensitive, confidential information, hard drives and other storage media must be properly disposed of when no longer in use. Hard drives should be physically removed and destroyed or wiped clean.
4. **Data backup.** Daily backups should be stored in a secure location. Weekly and fiscal year-end backups should be performed and stored at a secure off-site location.

5. **Disaster recovery.** A disaster recovery plan should be developed for personnel to follow in the event of a major hardware or software failure. The plan needs to be tested periodically to ensure effectiveness.
6. **Logical access.** Passwords are the first line of defense against hackers and others seeking unauthorized access to systems. Unique passwords should be assigned to each valid login.
7. **Physical access.** Access to an office and its computer resources should be restricted to individuals whose job responsibilities authorize such access.
8. **Virus/spyware.** The most efficient way to prevent viruses and spyware is to install virus and spyware prevention software. In addition to installing the software, current updates must be performed.
9. **Wireless security.** Wireless networks should have proper security in place. The county should configure the wireless access points or routers to implement established security protocols. Logins and passwords should be required.
10. **Web-based applications.** The county should design and implement web-based applications that address security vulnerabilities to protect secured information being passed back and forth on the Internet.

Through technology audits, the Division of County Audit helps ensure proper controls are in place for information systems. "Lack of information system control could jeopardize a county's data accuracy and financial and operating statement reliability," said Jim Arnette, assistant director of information systems.

"There are numerous offices in county government and these risks would apply virtually to any office," Alexander said. "We hope this guide helps county offices look at their own systems to see if they are vulnerable to risks."

The Division of County Audit is presenting "High Risk Areas Involving Technology in County Governments," at the County Officials Association of Tennessee and the Tennessee County Services Association conferences in October. County officials can also view the guide on the Comptroller's website, www.comptroller.state.tn.us/cpdivca.htm.

The Division of County Audit is responsible for annual audits of Tennessee's 95 counties. Division staff currently conduct audits in 89 counties. Audits in the remaining six counties are conducted by private certified public accountants (CPAs). These audits include the various offices, departments and entities of county government. County Audit is one of 13 divisions within the Comptroller of the Treasury whose mission is to improve the quality of life for all Tennesseans by making government work better.

###