



STATE OF TENNESSEE  
COMPTROLLER OF THE TREASURY  
DEPARTMENT OF AUDIT  
DIVISION OF COUNTY AUDIT

July 2006

## HIGH RISK AREAS INVOLVING TECHNOLOGY IN COUNTY GOVERNMENTS

The following high risk areas involving technology in county governments have been identified by the Division of County Audit's information systems audit staff. The weaknesses have been ranked in order of potential risk:

### What Determines a High Risk Area?

The Comptroller of the Treasury, Division of County Audit's information system reviews identify general control and application control weaknesses. Many of these weaknesses are considered to be high risk due to their potential to lead to fraud, waste, abuse, and mismanagement. These high risk areas jeopardize data accuracy and financial and operating statement reliability.

### Solution

In this document, the Division of County Audit summarizes each high risk area and provides a recommendation on what needs to be done to address the weakness. The Division encourages county governments to address these high risk areas and will continue to monitor a county's compliance efforts through the information system review process.

#### 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. This lack of application control could allow inappropriate system activity. Users could delete or alter the receipts that were paid with cash and take the money. No evidence of the original receipts would exist within the application and the deposit listings and reports would appear complete.

Any changes to previously issued receipts should be made through a void option that retains the original receipt information. An alternative control would be an audit log that records all deletions or alterations. For this log to be an adequate compensating control, it must be evaluated by management on a regular basis.

#### 2. Segregation of Duties

Duties relating to automated accounting functions are often not adequately segregated. One individual receipts collections, maintains accounting records, reconciles bank statements, prints reports, and signs checks. Inadequate segregation of duties significantly weakens the internal control structure. Employees with incompatible responsibilities could misappropriate funds without anyone's knowledge.

Ideally, incompatible duties should be segregated to strengthen internal controls. However, we realize that due to limited resources and personnel, management may not easily segregate these duties among employees. When segregation is not feasible, management should take a more active role in reviewing transactions and reports.

#### 3. Hardware Disposal

Computer hard drives and other storage media are not properly disposed of when no longer in use. There are several county offices that store sensitive, confidential information on their computers (i.e., employee social security numbers, medical information, and court records). This information is not considered public record and should be guarded with great care. If this type of sensitive information is not removed from a county computer that is sold or moved to surplus property, the information could fall into the wrong hands and be used inappropriately.

In order to prevent someone from obtaining this information, hard drives and other storage media must be properly disposed of when no longer in use. The hard drive should be physically removed and destroyed or wiped clean with reliable wiping software.

For more information, contact Penny Austin at (615) 401-7841 or Penny.Austin@state.tn.us.

Division of County Audit

## HIGH RISK AREAS INVOLVING TECHNOLOGY IN COUNTY GOVERNMENTS (Cont.)

### 4. Data Backup

Deficiencies in computer system back-up procedures exist. Daily backups are not performed and stored in a secure location within the office. Unsecured access to backups exposes the data to environmental hazards, as well as to possible sabotage. Weekly backups are not stored at a secure, off-site location. An off-site storage location is critical because, in the event of a disaster, all back-up data could be destroyed, resulting in costly delays in generating and recording information accounted for through the automated process.

A backup labeled for each day of the week should be maintained. Daily backups should be stored in a secure location. In addition to daily backups, weekly and fiscal year-end backups should be performed. Weekly back-up tapes should be rotated off site on a weekly basis while fiscal year-end backups should be retained off site indefinitely. Also, a current log of all backups that includes label descriptions, date of creation, contents, and storage location should be maintained.

### 5. Disaster Recovery

Disaster recovery plans have not been developed. Disaster recovery planning is necessary to minimize loss and ensure continuity of the critical business functions of an office in the event of disaster.

A plan should be developed for personnel to follow in the event of a major hardware or software failure, or temporary or permanent destruction of facilities. This document should outline what needs to be done, who is going to do it, and in what order it will be done. This plan should be updated on a regular basis and stored at a secure off-site location. The plan needs to be tested periodically to be sure that it is both complete and effective.

### 6. Logical Access

Logical access controls are inadequate. In some instances, passwords are not assigned to operating system or application user logins. If passwords are used, they are not changed regularly. Also, logins and passwords of former employees may remain active on the system. Logins used by the public to access information are not always restricted to inquiry-only access. Inadequate controls over the access to the software applications and operating system exposes the office to the unauthorized access to and manipulation of sensitive automated financial information.

Passwords are the first line of defense against hackers and others seeking unauthorized access to systems. Therefore, unique passwords should be assigned to each valid login. These passwords should remain confidential and should be changed periodically. Furthermore, the user logins assigned to former employees should be removed from the system. Public access should be restricted by using inquiry-only logins.

### 7. Physical Access

Controls over the physical access to computer systems are inadequate. Computers are located in areas that are easily accessible to unauthorized individuals. On occasion, officials will allow individuals to have access to the office after business hours. Allowing persons who are not employees to have unsupervised access to computer systems seriously weakens internal controls over office assets. Unrestricted physical access exposes an office's computer resources to the unauthorized use of computer hardware, system modifications, physical damage, and theft.

Officials should implement access controls to protect their offices and computer resources from unauthorized use. Access to an office and its computer resources should be restricted to individuals whose documented job responsibilities authorize such access.

## HIGH RISK AREAS INVOLVING TECHNOLOGY IN COUNTY GOVERNMENTS (Cont.)

### 8. Virus/Spyware

Computer systems are not adequately safeguarded against computer viruses and spyware. Malicious computer code can be attached to emails, stored on external storage media, or obtained in many other ways. New viruses are released almost daily and can cause serious problems in a computer system. Some viruses completely shut down a system so that it is no longer usable until the operating system is reloaded and the virus is eliminated. Spyware is downloaded on the computer without the knowledge of the user and comes in many forms that can cause various levels of harm. Spyware can cause problems as simple as slowing down the computer or as vicious as recording each keystroke a user makes. Once installed, spyware can monitor user activity, gather information about email addresses, passwords, and credit card numbers, and transmit this information to someone else. If an office does not implement measures to protect its system against these threats, loss productivity or theft of information could result.

The most efficient way to prevent viruses and spyware is to install virus and spyware prevention software. This software will constantly monitor computers for worms, viruses, Trojans, and spyware and then block, remove, or quarantine those threats. Several of these programs are offered as free downloads from the Internet or may be purchased from a vendor. In addition to installing the software, current updates must be performed. The updates assist in protecting the system from newly released viruses. Users must use the Internet with caution by not opening emails from unknown users or visiting inappropriate sites.

### 9. Wireless Security

The rapid introduction of wireless functionality is convenient and a significant security threat. Wireless networking uses an access point or a wireless router to provide network connectivity to any computer with a compatible wireless access device. Any computer inside or outside the county's control with a compatible wireless access device could access the county's network. If security over the wireless network is not properly configured, an unauthorized individual could gain access to the county's network and cause problems by accessing applications and sensitive files or performing attacks against other computers via the Internet using the county's network as the platform.

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 to gain access to the network. The county should monitor their network for unauthorized wireless access points and disconnect or secure them if found.

### 10. Web-Based Applications

Proper controls over web-based applications may not exist. These applications are accessed by using a web browser such as Windows Explorer or Mozilla to log on to a secured website. The security and monitoring of the site determines the security of the county's data. Web-based applications also garner concerns regarding the security of information being passed back and forth on the Internet as well as the ownership and portability of the data. Data related to the web-based applications may be corrupted due to the lack of controls over user authentication and Internet communications. Web-based applications could also inadvertently allow access to the confidential information exposing the county's customers to potential identity theft issues.

The county should design and implement web-based applications that address web-based application security vulnerabilities that have been outlined in many industry projects and publications. The county, in addition to proper web-based application design, should scrutinize user authorization capabilities and monitor the application to identify suspicious activity.