Internal Control Risks Associated with Information Technology

By

Kevin M. Bronner, Ph.D.

Introduction: The Risk of Information Technology Fraud

The information technology (IT) function is important to many organizations in the United States and abroad. One of the first questions to be asked in fraud assessments is what is the risk associated with information technology? For many years I served as an auditor and have also taught accounting and auditing courses. These courses include a course in detecting fraud and forensic accounting techniques. The Association of Certified Fraud Examiners (ACFE) has numerous publications that I have used in structuring these courses. For many years I have used the fraud information included in numerous issues of the Report to the Nations on Occupational Fraud and Abuse hereinafter (referred to as Report to the Nations).\(^1\)

The Report to the Nations illustrates that much of the fraud to be encountered is committed by the upper management of the organization, by members of the accounting department, or by people working in operations and in sales. These four groups are associated with the following percentage of fraud cases outlined in the report at page 61:

- Accounting 24.3%
- Operations 20.7%
- Executive/Upper Management 13.9%
- Sales 13.1%

We can see, therefore, that approximately 72 percent of the fraud detected is committed by these four departments. In many cases, however, the computer system is used by persons working in another office as a tool to commit fraud. The Report to the Nations shows that only 2.8 percent of the fraud is associated with the Information Technology in organizations in the United States. The Report to the Nations pp. 61-62 also shows that internationally the fraud cases involved with Information Technology function are: Asia (1.5%), Europe (4.1%), Africa (2.9%), Canada (4.5%), Oceania (5.3%), and Central/South America and Caribbean (1.5%). The information technology internal control recommendations discussed below can easily be adapted to international organizations.
The Office of the New York State Comptroller is headquartered in Albany, New York. It conducts an auditing function which produces audits of New York State local government agencies such as school districts, counties, towns, villages, and special taxing districts. These audits produce excellent case studies that can be used to illustrate fraud auditing techniques and the type of fraud that is uncovered. In many of these audits the management of the government manipulated the computer system to commit occupational fraud. In some cases the computer system was used to change the names of vendors or to produce false vendors or employees in order to structure transactions to steal the assets of the organization. A prime example of the use of the computer system to commit occupational fraud is found in the following audit: Office of the New York State Comptroller Roslyn Union Free School District Anatomy of a Scandal Report of Examination Report 2005M-21 (Roslyn audit).  

The Office of the New York State Comptroller audits have illustrated that managers who are not working in the information technology office can manipulate records if adequate computer system controls are not in place. Numerous problems can occur if employees are provided with access to the computer system if that function is not associated with their job. If too many users have access to the computer system, there is a loss of internal control since users who should not be able to make changes to the accounting records can easily manipulate the data. One audit conducted by the Office of the New York State Comptroller clearly illustrated that fraud was committed with employees with improper computer access authorization changed the names of 15 vendors with a cost of $6.2 million. If the user access to the computer system had been properly structured, most of this fraud could have been avoided.

During October 2010 the Office of the New York State Comptroller issued a new publication entitled The Practice of Internal Controls. This publication provides recommendations to limit fraud in local governments including an extensive section on information technology controls. The publication draws on the experiences of the numerous audits that have been conducted by the New York State Comptroller over the years. The Practice of Internal Controls document (p. 1) calls special attention to internal control in the information technology sector:

“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...”
While the *Practice of Internal Controls* document discusses internal controls in many areas such as cash receipts and disbursements, bank account reconciliations, and payroll and procurement, this article focuses on the area of information technology controls.

**Office of the New York State Comptroller October 2010 Information Technology Recommendations**

The Office of the New York State Comptroller report has produced 66 detailed recommendations on how the information technology function in a local government can be enhanced to improve internal controls. The recommendations are organized into eight program areas and include the following categories and number of recommendations:

1. Establishing the IT Framework (5 recommendations)
2. Protecting User Accounts (14 recommendations)
3. Monitoring Computer Users (6 recommendations)
4. Data Security (7 recommendations)
5. Software Security (6 recommendations)
6. Network Security (13 recommendations)
7. Physical Security of the System (8 recommendations)
8. Service Continuity of the System (7 recommendations)

While space limits prohibit a full discussion of all 66 information technology recommendations, eight of the recommendations are discussed below. These recommendations are all from the “Protecting User Accounts” and in the “Monitoring Computer Users” area of the *Practice of Internal Controls* report.

The New York State Comptroller has conducted a number of audits over the years. Some of the audits illustrated that employees made changes to the computer system even though they should not have had access to the system. These changes resulted in a misuse of the accounting system so the employees could steal assets from the organization. The reader is encouraged to review the full *Practice of Internal Controls report* including all the information technology recommendations and other recommendations that are included in the report. As stated above, the *Practice of Internal Controls report* also has numerous internal control
recommendations in other areas such as cash receipts and disbursements, bank account reconciliation procedures, billing and procurement issues, payroll and other items.

Eight Specific Information Technology System Recommendations

The following eight recommendations were developed by the Office of the New York State Comptroller in their internal control report. Each of the recommendations is briefly discussed below.

1) **Recommendation 9-2-2**: Ensure all users have a unique user name.

   This recommendation is necessary since all changes to the computer system can be traced to a specific individual in the organization. A number of audits conducted by the State Comptroller found that employees working in the management and accounting area had changed accounting transactions to commit occupational fraud. It is easier to determine who is committing the fraud if each employee is assigned an individual user account.

2) **Recommendation 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.

   This is necessary to ensure that employees and contractors who have left the service of the organization can not alter or delete data or otherwise change programs. Also, dormant accounts can not be used by others to commit fraud.

3) **Recommendation 9-2-6**: Use an authentication system to log-on to the network and specific applications.

   This recommendation is useful since 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. Examples of a biometric test may include items such as eye or fingerprint scanners or voice recognition software. The use of these controls reduces the risk that unauthorized users will change system data to commit occupational fraud. Several audits conducted by the Office of the State
Comptroller show that data such as vendor names had been changed by unauthorized users.

4) **Recommendation 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.

There is risk that computers that are logged on and not monitored can be used by other employees to change data. An additional layer of computer security is provided when the computer is shut down.

5) **Recommendation 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.

Limiting access to data bases and the computer system will ensure that employees who don’t have any function involved in the system will not be able to access the data. In the past the Comptroller’s audits found that users who had no valid job function related to the data bases had changed the system to commit occupational fraud.

6) **Recommendation 9-3-2**: Monitor user access into the network.

This recommendation is designed to examine unusual activity on the computer network. For example, if system users are logged on at unusual times such as very late at night or on weekends, or if there is an unusually high amount of error messages related to improper use of passwords, there could be a problem.

7) **Recommendation 9-3-3**: IT administration should use a web filter and review logs it creates.

A web filter is a tool used by management to monitor websites visited by system users. Administrators should use a web filter since it may detect web sites visited by employees involved with potential fraud. For instance, an employee setting up a false company for illegal purchasing activities may visit the web sites of vendors as part of the scheme.

8) **Recommendation 9-3-4**: Review audit logs of the applications, including the financial software.
Audit logs record certain activity associated with software such as changes to a database. For example, an audit log may show that on December 3, 2010 at 11:00 am user #23465 on the system changed the hourly earnings rate of employee #1245. Information Technology administration should review audit logs to ensure that only authorized users are making changes to the database. If unusual or unauthorized activity is indicated by the audit logs, an internal control problem may exist.

**Summary and Conclusions**

Information technology (IT) functions have unique internal control risks for the organization. The Office of the New York State Comptroller conducted hundreds of audits over the years. A number of these audits illustrated that the management of some local governments committed occupational fraud by stealing assets from the organization. In some cases weaknesses in the information technology system were used by employees to make changes to the computer system. During October, 2010 the Office of the New York State Comptroller produced 66 specific recommendations relating to enhancing the security of the information technology function for local governments. Many of these recommendations provide common sense solutions that can be used by fraud auditors and those involved with internal controls to help protect the assets of the organization. The recommendations can be used for those auditing entities in the private sector and in the public sector. Also, the information technology internal control recommendations can be applied to organizations at the international level.

---

