Unauthorized access can lead to devastating effects. Entities can become victims of malicious activities such as identity theft, financial fraud, theft of data (e.g., credit card data) and attacks on systems (e.g., denial of service), which can be especially harmful for online businesses. All of these harmful effects have been the subject of various news reports in the past.

Criminals, especially IT-savvy ones, have become expert at recognizing weaknesses in access and have become knowledgeable about the tools necessary to successfully exploit weak systems. In fact, experts say more and more criminals are focusing on IT crimes rather than traditional street crimes. Statistics from the Computer Emergency Readiness Team (CERT) and industry security analysts show that about 80 percent of all malicious activities come from current or former employees.¹

Thus, more than ever, one of the prime concerns in any audit, and for management, is the logical access to computer systems and data. The proliferation of IT, and the Internet in particular, has caused the risks associated with systems and data to explode. In fact, this topic has made the American Institute of Certified Public Accountants (AICPA)’s Top Technology Initiatives every year since 2005 and is ranked first on the 2010 list.² Some level of audit risk and business risk exists in virtually every audit because of a variety of IT-related vulnerabilities, but especially access controls.

Earlier this year, this column identified five areas of IT general controls (ITGC) that should be examined in every financial audit.³ Logical access was one of those five. This article adds further information, in a broader sense of audits, about logical access.

To mitigate the risks associated with access control, it is necessary to identify the risks associated with access controls and to assess the level of those risks. An entity must then establish sound policies and procedures for granting authorized users access while simultaneously protecting itself from unauthorized access. This area of concern is generally considered a subset of identity and access management (IAM). One method for addressing these risks is through the perimeter for authorized access, the process of granting access on only a need-to-know basis (including admin rights) and the process of terminating employees.

MITIGATING LOGICAL ACCESS RISKS

On the perimeter, best practices include authorization and authentication of users in the access rights policies and procedures.

Authorization access controls are those with an objective to ensure that the person seeking access is authorized. This control is most often associated with login credentials and procedures, e.g., requiring an ID and password. However, the hacker world has developed sophisticated tools that can break fairly easily into systems with unsophisticated passwords (names, words found in the dictionary, etc.). Therefore, over the years, best practices have been expanded to include “strong” passwords, frequent changes to passwords and multifactor access controls, as appropriate. The greater the risk, the greater the need for more sophisticated and secure access, and the greater the need for additional layers of access controls. The more of the following elements a password includes, the stronger it is considered to be:

• It is at least eight characters long.
• It includes at least one special character.
• It includes at least one number.
• It mixes cases for alpha characters.
• It uses an incoherent phrase (i.e., not an address, etc.).

The purpose of these elements is to thwart existing hacker tools that can guess passwords. Weak passwords and PINs are the major cause for security breaches, according to IT consulting firm Frost & Sullivan.⁴ Usernames and passwords/PINs are usually static or shared across multiple accounts by users, making them

¹ISACA JOURNAL VOLUME 5, 2010

²ISACA JOURNAL VOLUME 5, 2010

³ISACA JOURNAL VOLUME 5, 2010

⁴ISACA JOURNAL VOLUME 5, 2010
Employees should have access to only those applications and data necessary for that person's job responsibilities. That limitation also includes data access rights of read-only, read/write or no access, where applicable (i.e., need-to-know access). For instance, a good security policy would be to have a strong logical access system on the network to log in to the system (e.g., Active Directory applied effectively on Microsoft SQL Server). But then, where risks are high, the entity should have another system of login credentials and access granted for each key application. Some application systems, such as Microsoft Dynamics, provide their own access control as a separate layer of security over data access via the applications. If both of these access control systems are managed properly, someone’s ability to break through the perimeter can be mitigated by strong access controls in the “back office” system—that is, a strong pair of controls to prevent unauthorized access. This need-to-know approach to applications is a key element of sound access controls.

Administrative access rights are a critical area that need controls because of the broad access rights “admin” has once logged into the system, and they are included as part of “need to know.” Adequate access controls should provide for the application of best practices for the administrator function of databases or database management systems (DBMS), such as DB2, Oracle and SQL Server. They include, but are not limited to, not using a default ID/password for admin, minimizing the number of employees with admin access and establishing some modicum of segregation of duties. Admin rights are especially critical for operating systems in which root access can be granted, giving someone “the keys to the kingdom.” Obviously, this area is another that should be examined during most IT audits of any nature.

Lastly, when employees are terminated, there should be effective controls in place to terminate the employee’s access to the systems. At termination, entities sometimes forget about logins and access rights formally granted to employees. All entities need an effective control or set of controls to ensure that all terminated employees lose all access rights.

An effective and logical approach is to tie access control to human resources (HR) procedures. When an employee is hired, transferred or leaves the organization, the HR procedures should include the requisite changes to that employee’s access rights. When a new employee is hired, that person’s “need to know” should be assessed and access rights should be granted to only those applications and data necessary for that person’s job responsibilities. Either the
application or the network software should have the means to limit access appropriately. If an employee is transferred, those access rights may change because of the different responsibilities involved in the transfer. Thus, the HR transfer process should include a review of and a change, if necessary, in access rights. When an employee leaves the organization for any reason, but especially if the employee is fired, access rights should be terminated as close to the person’s termination as possible, but no later than the person’s last day on the job.

CONCLUSION
The IT auditor should consider the previously disclosed procedures in an audit to ensure that access controls are adequate to mitigate the risks associated with access, including limiting the access of legitimate employees to need to know, and mitigating the risk of an unauthorized intrusion.

ENDNOTES